Chapter 4: Wireless LANs

Table of Contents

Introduction

- New networking technologies and paradigms such as:
  - Wireless LANs (Local Area Networks)
  - Wireless PANs (Personal Area Networks)
  - Wireless MANs (Metropolitan Area Networks)
  - Wireless WANs (Wide Area Networks)
  - Wireless RANs (Radio Access Networks)
- Dominant choice:
  - Ad hoc and mesh (or infrastructureless) mode offered by the WLANs and WPANs technologies
  - For WLANs, IEEE 802.11 standard and their variations: the most well known representatives: discusssed in this chapter
  - IEEE 802.15 Working Group for WPANs: discussed in the next chapter

Why Wireless LANs?

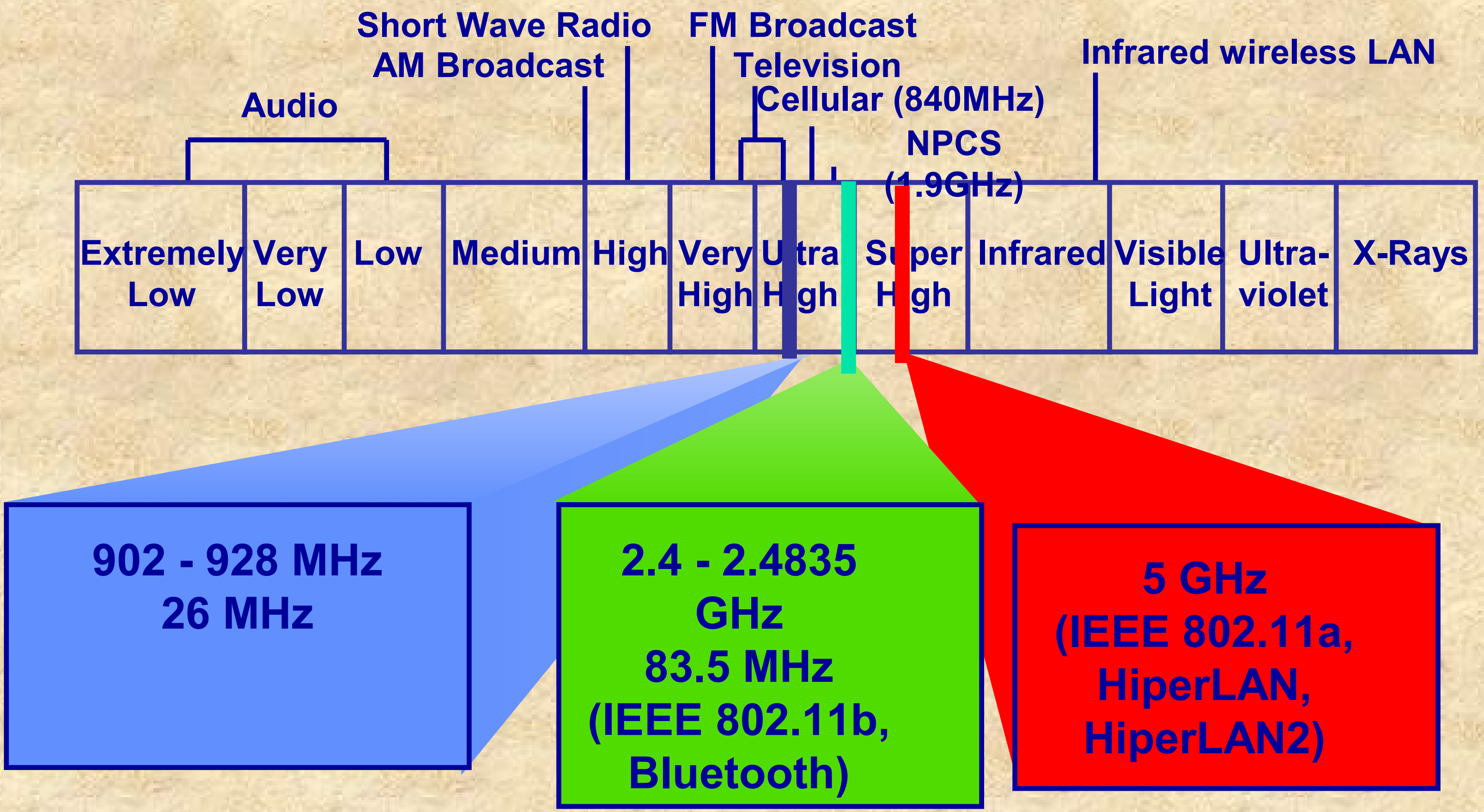
- **Ethernet Standard LAN protocol operates at a fairly high speed using inexpensive connection hardware**
- **LANs have been limited to the physical, hard-wired infrastructure of the building**
- **Many mobile users in businesses, medical profession, factories, and universities find many benefits from the added capabilities of wireless LANs**
- **Wireless LANs provide mobility and untethered from conventional hardwired connections**
- **Practical use of wireless networks is limited by an individual's imagination**
- **It may even be economical to use a wireless LAN in old buildings**

Transmission Techniques

- **We would like to transmit data with:**
  - **Highest possible data rate**
  - **With the minimum level of the signal power**
  - **Minimum channel bandwidth**
  - **Reduced transmitter and receiver complexity**
- **Wired**
  - **Data received from upper layers are line coded and the voltages are applied to the medium directly**
  - **Transmissions are often referred to as *baseband transmission schemes***
  - **In voice-band modems, Digital Subscriber Line (DSL), and coaxial cable model applications, the transmitted signal is modulated over a carrier**
- **Wireless: 3 categories**
  - **Pulse transmission techniques employed mostly in Infrared (IR) applications and, more recently, in the so-called impulse radio or ultra-wideband (UWB) transmission**
  - **Basic modulation techniques widely used in Time Division Multiple Access (TDMA) cellular, as well as a number of mobile data networks**
  - **Spread spectrum systems used in the Code Division Multiple Access (CDMA) and in wireless LANs operating in ISM frequency bands**

ISM Frequency Bands

- 22 MHz channel bandwidth
- Must implement spread spectrum technology
- Must operate at 500 mill-watts or less



Infrared (IR)

- Remote controls for TVs, VCRs, DVD and CD players use IR technology
- A direct line of sight of the transmitter needed in order to successfully establish communication link
- New diffused IR technologies can work without LOS inside a room
- Systems are simple to design and are inexpensive
- Use the same signal frequencies used on fiber optic links
- Systems detect only the amplitude of the signal, so interference is greatly reduced
- IR transmission can be aimed and range extended to a couple of kilometers and can be used outdoors
- It also offers the highest bandwidth and throughput
- The other way is to transmit omni-directionally and bounce the signals off of everything in every direction, which reduces the coverage to 30 - 60 feet
- IR signals cannot penetrate opaque objects
- IEEE 802.11 standard for high-speed diffused IR employs pulse-position-modulation (PPM) with a wavelength of 850nm–950nm and data rates of 1 and 2 Mbps

Microwave and Radio Frequencies

- **Microwave:**
  - **Operate at less than 500 milliwatts of power (MW)**
  - **Use narrow-band transmission with single frequency modulation mostly in the 5.8 GHz band**
- **Radio Frequency:**
  - **To link appliances that are distributed throughout the house**
  - **Can be categorized as narrowband or spread spectrum**
  - **Narrowband technology includes microwave transmissions which are high-frequency radio waves that can be transmitted to distances up to 50 Km**
  - **Not suitable for local networks, but could be used to connect networks in separate buildings**
  - **Transmitted signal in Subscriber Station occupies a much larger bandwidth than the traditional radio modems**
  - **Two basic techniques used: frequency hopping spread spectrum (FHSS) and direct sequence spread spectrum (DSSS)**

Spread Spectrum

- **Frequency Hopping Spread Spectrum:**
  - **Splits the band into many small subchannels (e.g., 1 MHz)**
  - **Signal then hops from subchannel to subchannel transmitting short bursts of data on each channel for a set period of time, called dwell time**
  - **Hopping sequence must be synchronized at the sender and the receiver or else, the information is lost**
  - **FCC requires that the band is split into at least 75 subchannels**
  - **Extremely difficult to intercept and gives a high degree of security**

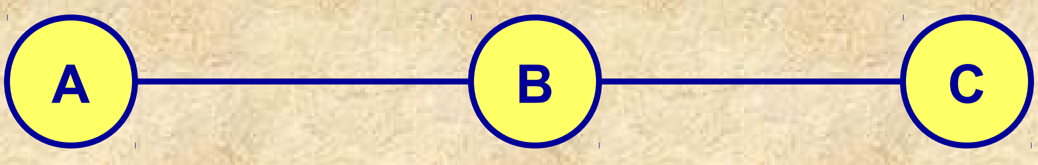
- **Direct Sequence Spread Spectrum:**
  - **Transmission signal is spread over an allowed band**
  - **Two-stage modulation technique: a random binary string, called the spreading code, is used to modulate the transmitted signal, and in the second stage, the chips are transmitted over a traditional digital modulator**

Direct Sequence Spread Spectrum

- Physical layer of the IEEE 802.11 standard employing DSSS requires a spreading ratio of eleven
- If orthogonal spreading codes are used, then more than one LAN can share the same band
- However, because DSSS systems use wide subchannels, the number of co-located LANs is limited by the size of those subchannels
- As the transmitted chips are much narrower than data bits, the bandwidth of the transmitted DSSS signal is much larger than systems without spreading
- The DSSS systems provide a robust signal with better coverage area than FHSS
- The DSSS systems provide a robust signal with better coverage area than FHSS

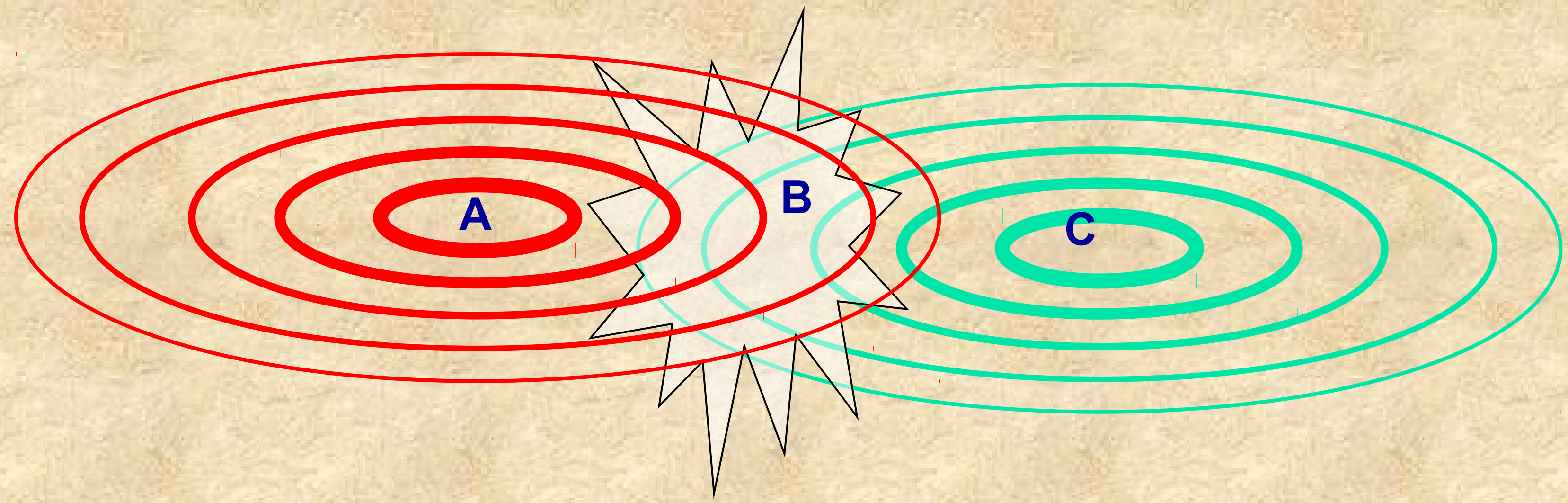
Medium Access Control Protocol Issues

- **Many issues need to be addressed in order to design an efficient MAC protocol**
- **Hidden Terminal Problem**



  - **Station A can hear B but not C, and station C can hear station B but not A**
  - **First, assume A is sending to B**
  - **When C is ready to transmit, it does not detect carrier and thus commences transmission; this produces a collision at B**

Hidden Terminal Problem

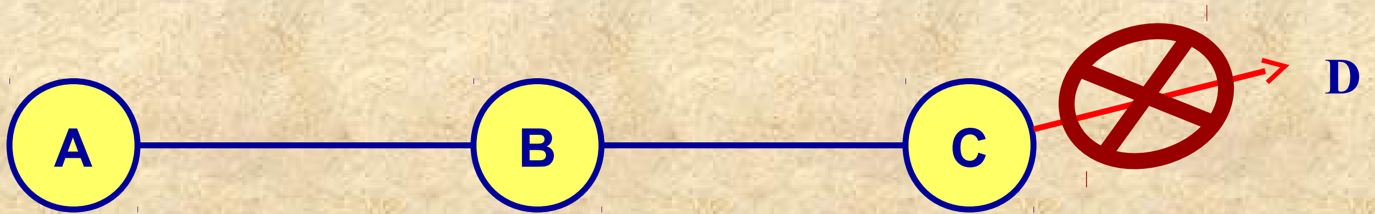


Hidden terminals

- **A sends to B, C cannot detect A's transmission**
- **C wants to send to B, C senses a "free" medium (CS fails)**
- **Collision at B, A cannot detect the collision (CD fails)**
- **A is "hidden" for C**

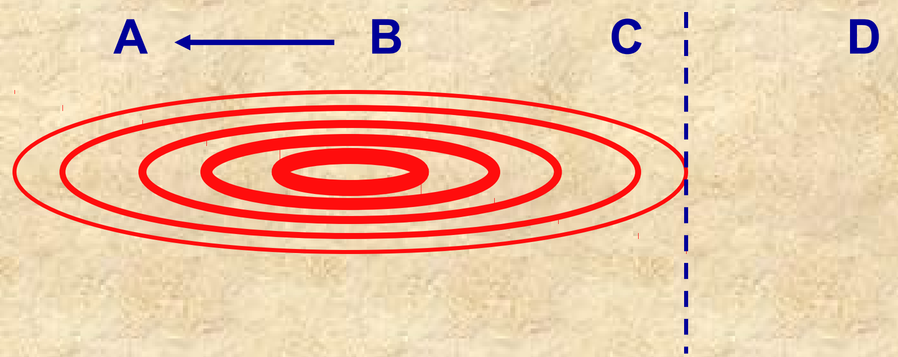
Medium Access Control Protocol Issues

- **Exposed Terminal Problem**



  - **Station A can hear B but not C, and station C can hear station B but not A**
  - **If we assume that B is sending to A rather than A sending to B**
  - **Then, when C is ready to transmit, it does detect carrier and therefore defers transmission**
  - **However, there is no reason to defer transmission to a station other than B since station A is out of C's range**
  - **Station C's carrier sense did not provide the necessary information since it was exposed to station B even though it would not collide or interfere with B's transmission**

Exposed Terminal Problem



Exposed terminals

- **B sends to A, C wants to send to D**
- **C senses carrier, finds medium in use and has to wait**
- **A is outside the radio range of C, therefore waiting is not necessary**
- **C is “exposed” to B**

Multiple Access with Collision Avoidance (MACA)

- MACA uses signaling packets for collision avoidance
  - RTS (request to send)

    -Sender request the right to send from a receiver with a short RTS packet before it sends a data packet
  - CTS (clear to send)

    -Receiver grants the right to send as soon as it is ready to receive

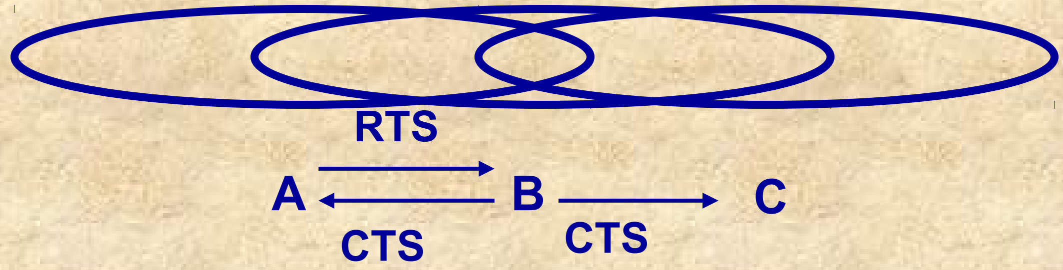
- Signaling packets contain
  - Sender address
  - Receiver address
  - Duration

Variants of this method are used in IEEE 802.11

MACA Solutions

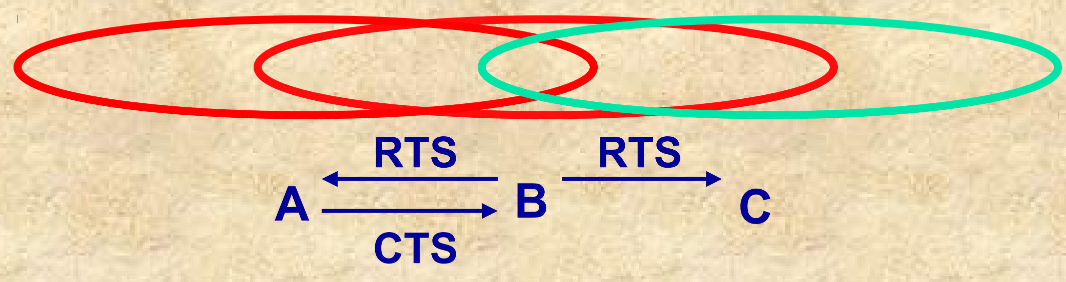
MACA avoids the problem of hidden terminals

- A and C want to send to B
- A sends RTS first
- C waits after receiving CTS from B



MACA avoids the problem of exposed terminals

- B wants to send to A, C to another terminal
- Now C does not have to wait, as it cannot receive CTS from A



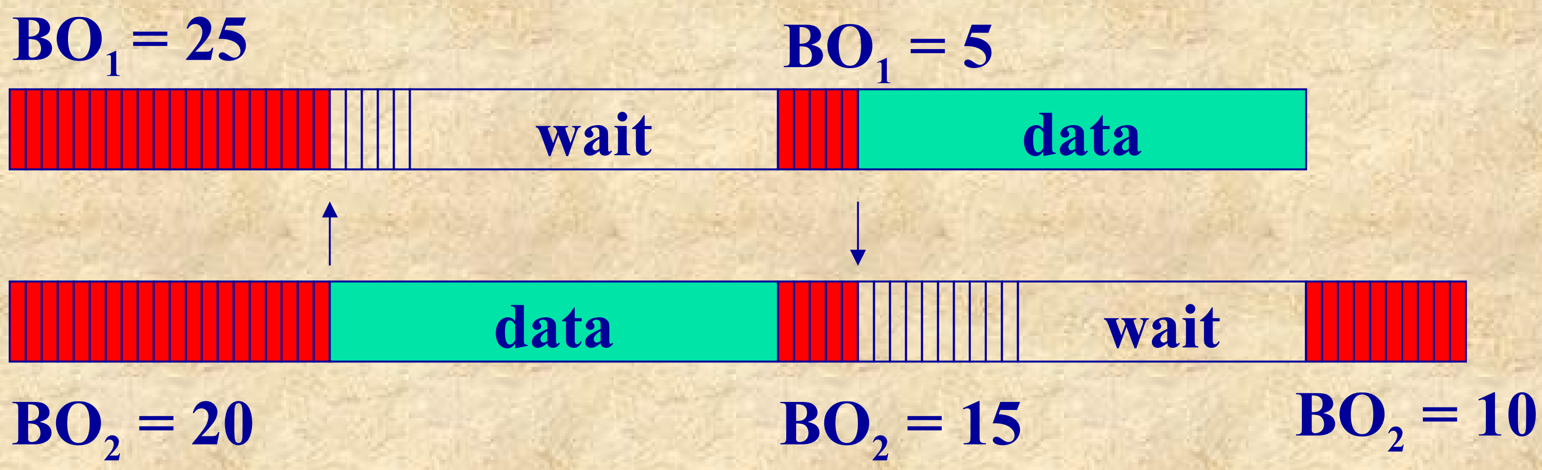
Medium Access Control Protocol Issues

- Solution to the hidden terminal problem proposed in the Medium Access with Collision Avoidance (MACA)
  - Transmitting Request-to-Send (RTS) and Clear-to-Send (CTS) packets
  - Stations in the neighborhood overhear either the RTS or CTS, keep quiet for the duration of the transfer
- Reliability
  - Packet error rates of wireless mediums are much higher than that of their wired counterparts
  - E.g., execution of TCP congestion control mechanism, a packet loss is erroneously assumed due to congestion and congestion control mechanisms are fired
  - This ultimately decreases the transmission rate, with the intention to reduce the network congestion
  - In wireless environment, packet loss occurs every now and then due to effects such as multipath fading, interference, shadowing, distance between transmitter and receiver, etc.
  - A common approach to reduce packet loss rates experienced by upper layers is to introduce acknowledgment (ACK) packets

Medium Access Control Protocol Issues

- Collision Avoidance
  - To minimize collisions, wireless CSMA/CA MAC protocols often use collision avoidance techniques in conjunction with a carrier sense
  - Collision avoidance is implemented by making node wait for a randomly chosen duration before attempting to transmit after the channel is sensed idle
- Congestion Avoidance
  - When a node detects the medium to be idle, it chooses a backoff interval between [0, CW], where CW is called contention window
  - CW usually has a minimum (CW_min) and maximum value (CW_max)

Congestion Avoidance



CW = 31

BO_1 and BO_2 are backoff intervals at nodes 1 and 2

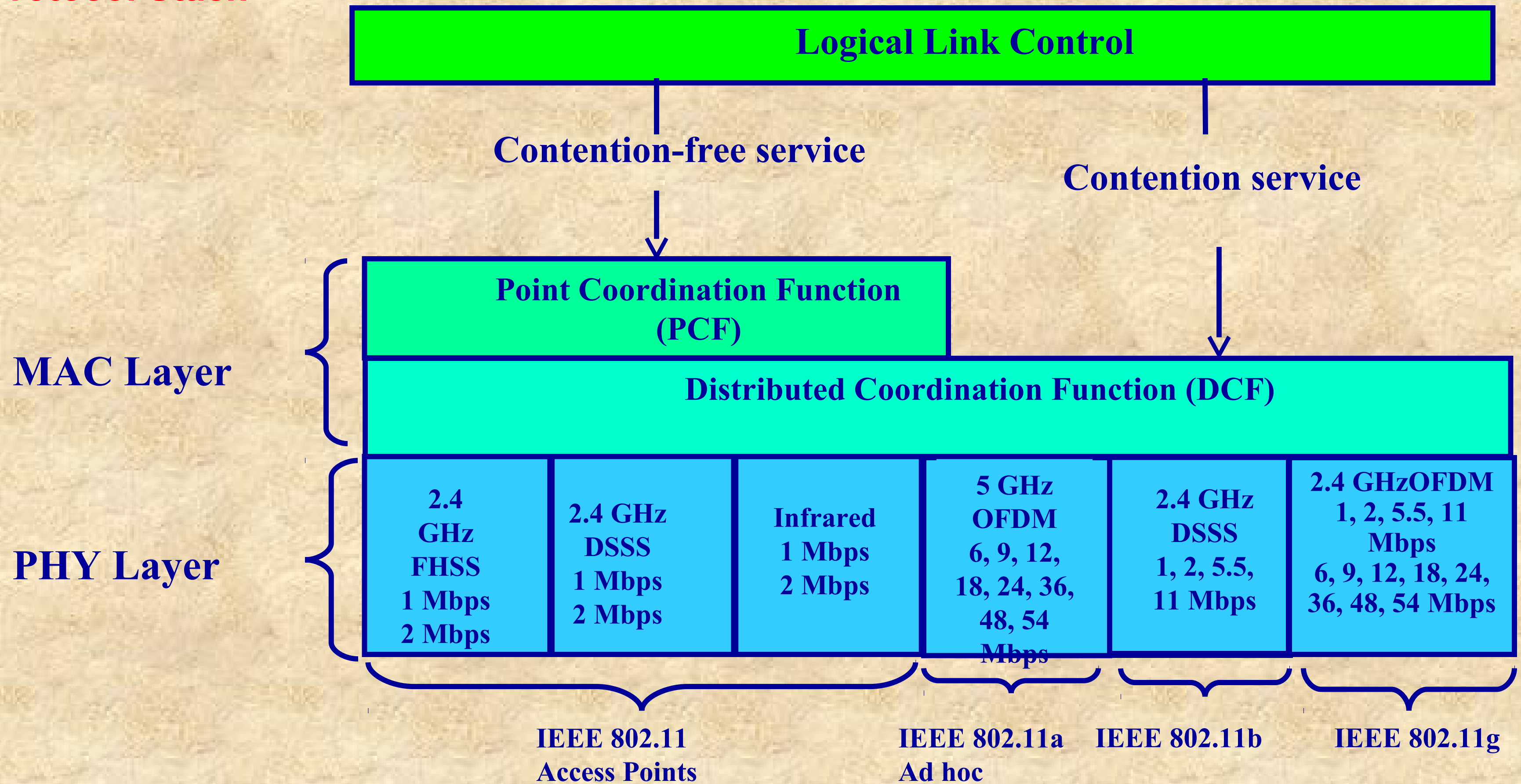
- BO_1 and BO_2 are the backoff intervals of nodes 1 and 2
- We assume for this example that CW = 31
- Node 1 and node 2 have chosen a backoff interval of 25 and 20, respectively
- Node 2 will reach zero before five units of time earlier than node 1
- When this happens, node 1 will notice that the medium became busy and freezes its backoff interval currently at 5
- As soon as the medium becomes idle again, node 1 resumes its backoff countdown and transmits its data once the backoff interval reaches zero

Medium Access Control Protocol Issues

- **Other MAC Issues**
  - **Many other issues need to be considered such as *fairness***
  - **Fairness has many meanings and one of them might say that stations should receive equal bandwidth**
  - **Unfairness will eventually occur when one node backs off much more than some other node in the same neighborhood**
  - **MACAW's solution to this problem [Bharghavan1994] is to append the contention window value (CW) to packets a node transmits, so that all nodes hearing that CW, use it for their future transmissions**
  - **Since CW is an indication of the level of congestion in the vicinity of a specific receiver node, MACAW proposes maintaining a CW independently for each receiver**
  - **All protocols discussed so far are sender-initiated protocols**
  - **In other words, a sender always initiates a packet transfer to a receiver**
  - **The receiver might take a more active role in the process by assisting the transmitter in certain issues such as collision avoidance, and some sort of adaptive rate control**

IEEE 802.11 Standard for Wireless LANs

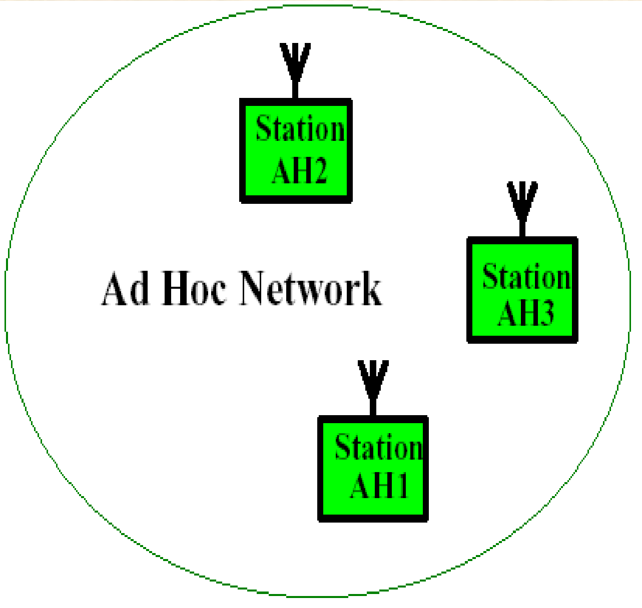
Details of 802.11 Protocol Stack



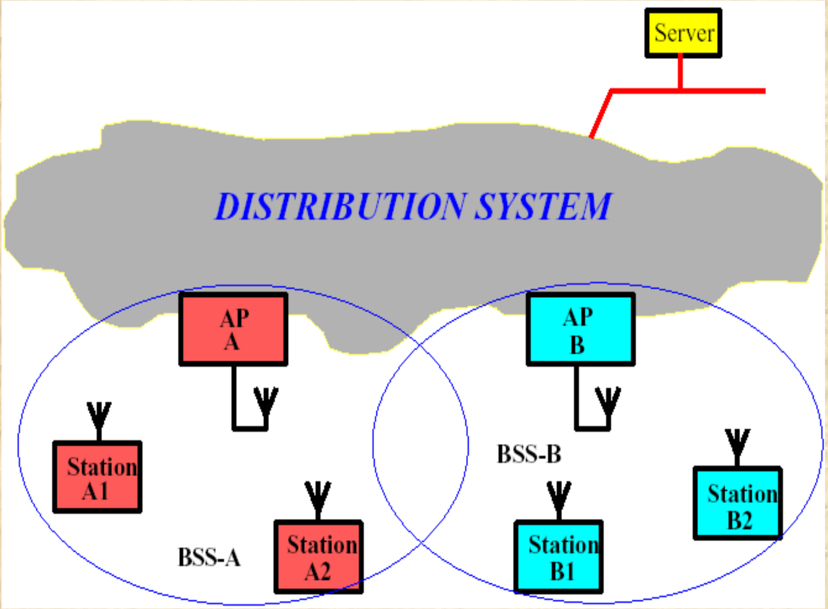
802.11 Protocol Architecture

Configuration:

- **To Replace Wired LAN**
- **Extension of Wired LAN Infrastructure**



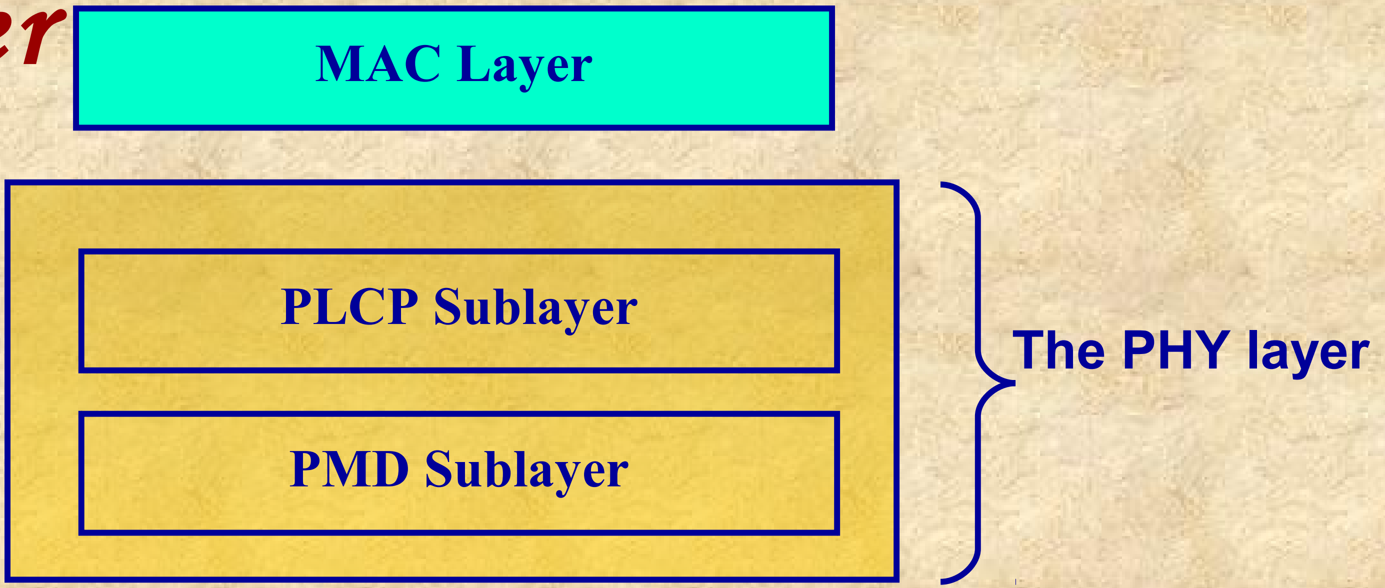
Replace Wired LAN



Extension of Wired Infrastructure

Possible Network Topologies

Sublayers within Physical Layer

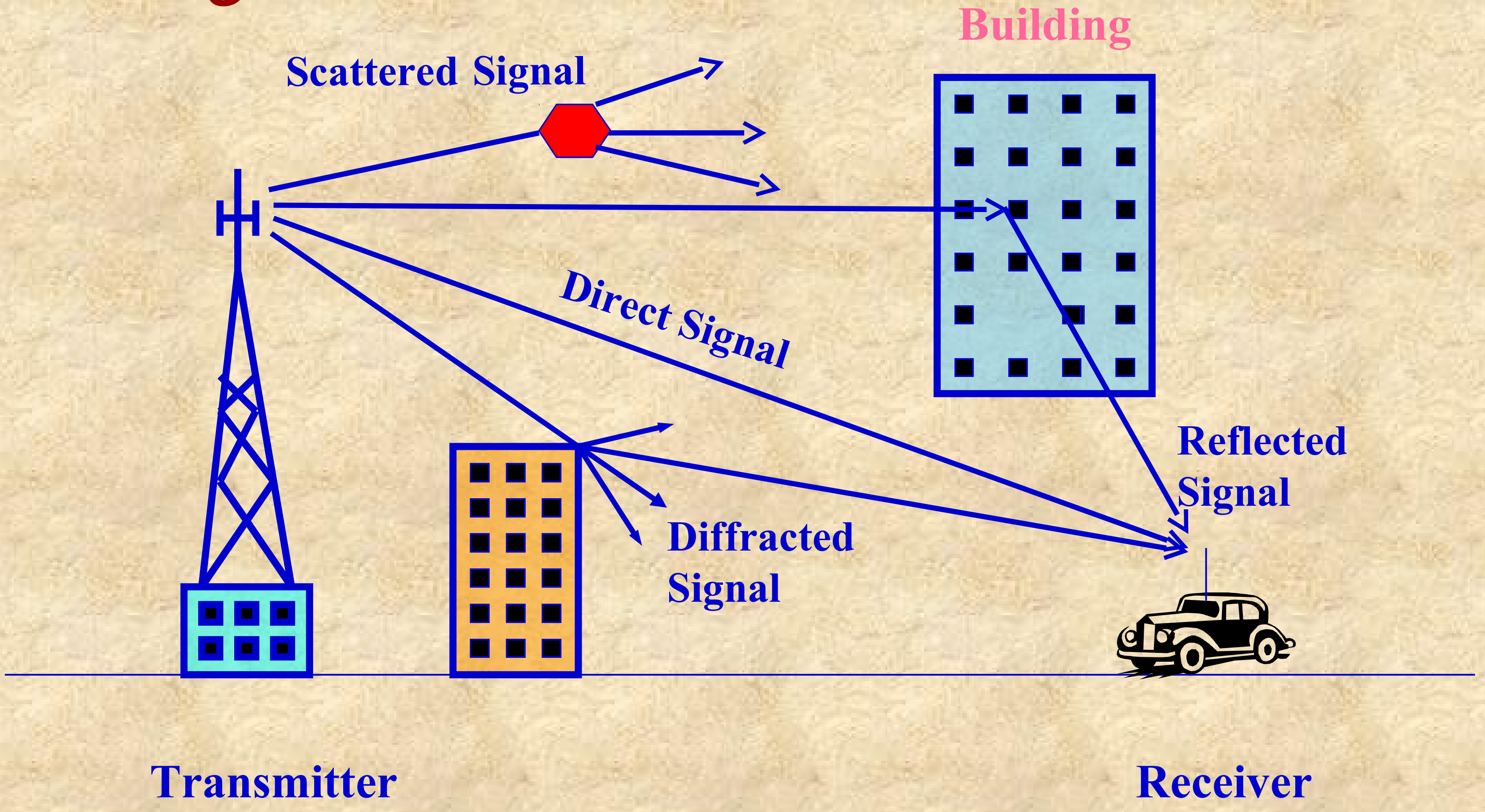


- PHY layer is the interface between the MAC and wireless media
- Provides three levels of functionality
  - Frame exchange between the MAC and PHY
  - Uses signal carrier and spread spectrum modulation to transmit data frames over the media
  - Provides a carrier sense indication back to the MAC

Limiting factors for high-speed Network Performance

- **Limiting factor for speed is the fast fading due to multipath propagation**
- **Fading between the transmitter and the receiver caused by:**
  - **Atmospheric scattering**
  - **Reflection**
  - **Refraction or diffraction of the signal**
  - **Causes signal to arrive at the receiver with different delays and interfere with itself causing inter-symbol interference (ISI)**

Multipath Propagation of Radio Signal



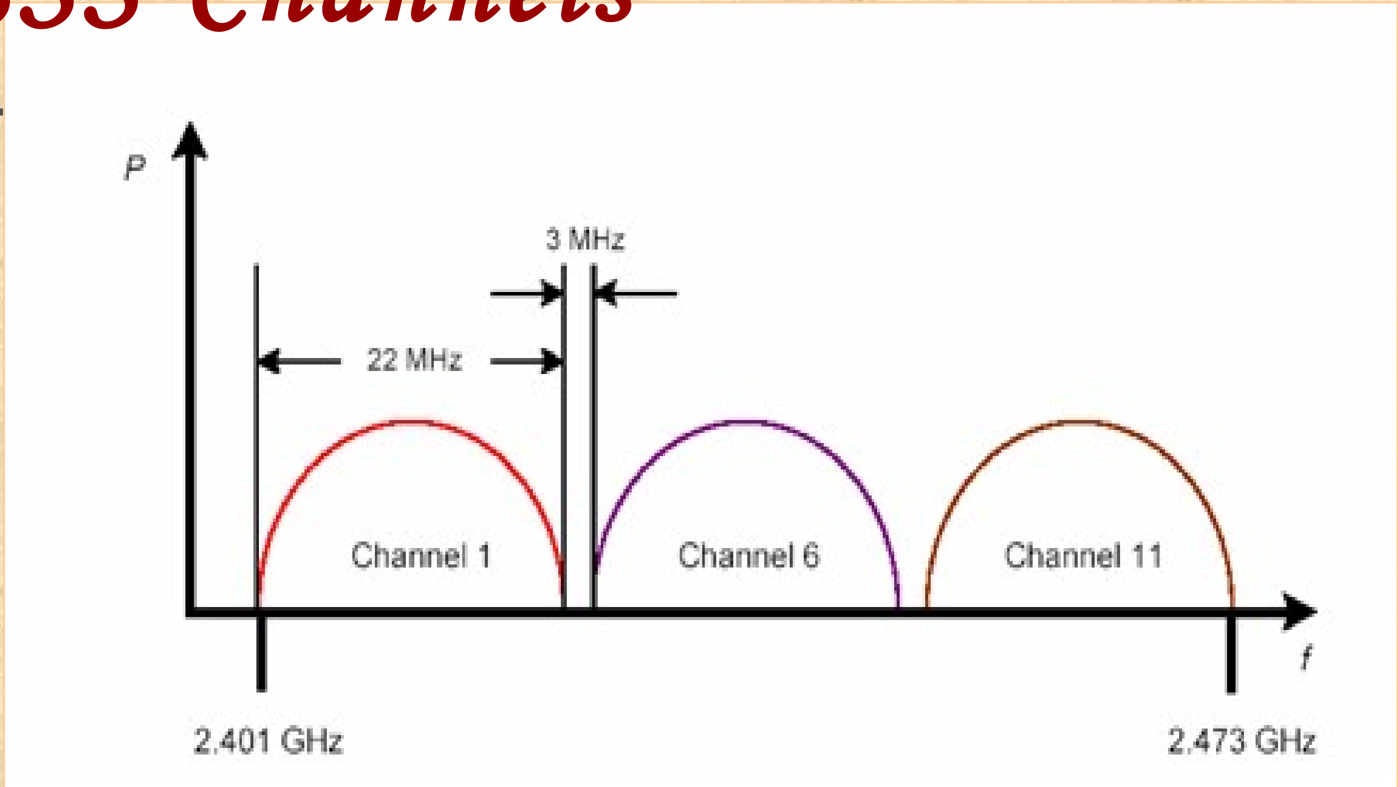
Frequency Selective Fading

- Frequency selective fading can be overcome by Spread Spectrum (FHSS or DSSS) and OFDM:
  - In Spread Spectrum, signal is processed in to occupy a considerably greater bandwidth to lessen the impact of frequency selective fading
  - In OFDM, the data stream is split into a certain number of substreams, each having a bandwidth smaller than the coherence bandwidth of the channel
  - GFSK is a modulation scheme in which the data are first filtered by a Gaussian filter in the baseband, and then modulated with a simple frequency modulation
  - DBPSK is a phase modulation scheme using two distinct carrier phases for data signaling, providing one bit per symbol
  - DQPSK is a type of phase modulation using two pairs of distinct carrier phases, in quadrature, to signal two bits per symbol
- A third physical layer alternative not widely used, is an infrared system using near-visible light in the 850 nm to 950 nm ranges as the transmission medium

IEEE 802.11 Standard

- Three supplements to the IEEE 802.11 standard: 802.11a, 802.11b and 802.11g, as well as an ETSI standard HIPERLAN/2
- Both 802.11a and HIPERLAN/2 operate in the 5 GHz band and use the modulation scheme OFDM, but the MAC layers are considerably different
- Compare physical layer characteristics of the IEEE standards 802.11a and 802.11b
- HIPERLAN/2 shares several of the same physical properties as 802.11a, and 802.11g

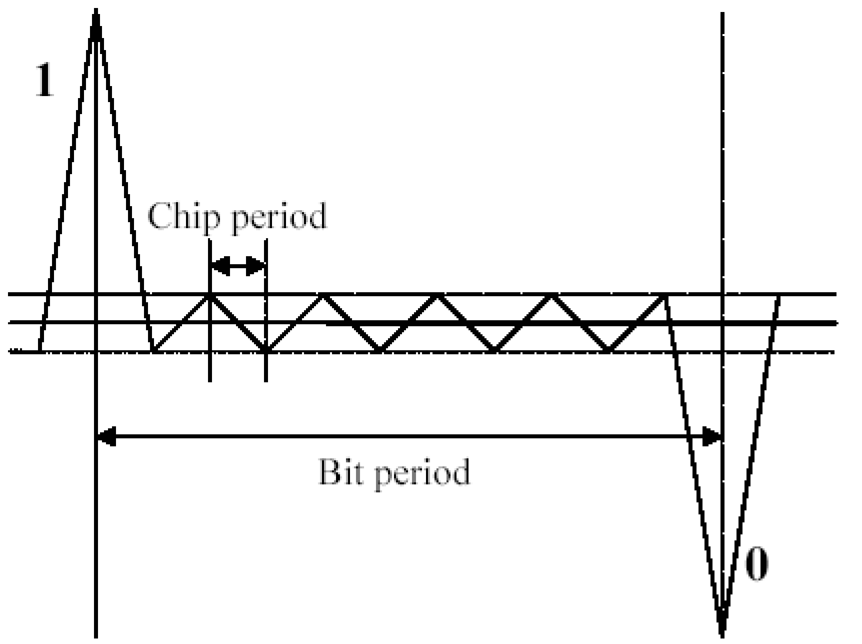
DSSS Channels



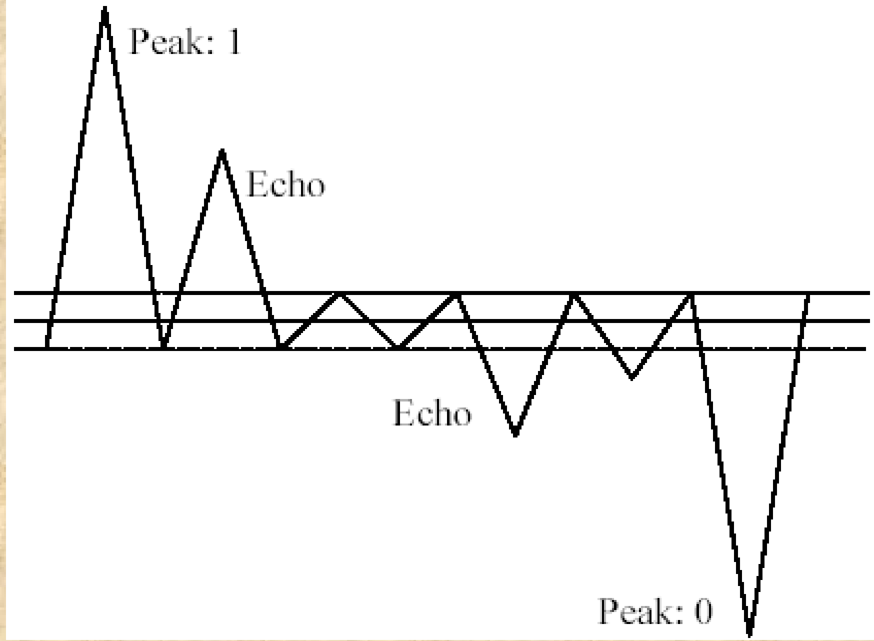
- **DSSS uses the 2.4 GHz frequency band**
- **IEEE 802.11 implements DSSS to fight frequency-selective fading**
- **The IEEE 802.11b supports 5.5 and 11 Mb/s of higher payload data rates in addition to the original 1 and 2 Mb/s rates of IEEE 802.11**
- **IEEE 802.11b also operates in the highly populated 2.4 GHz ISM band (2.40 to 2.4835 GHz), which provides only 83 MHz of spectrum to accommodate a variety of other products, including cordless phones, microwave ovens, other WLANs, and WPANs such as Bluetooth**
- **Maximum allowable radiated emission limited to 100 mW**

IEEE 802.11 and the 11-Chip Barker Sequence

- 11-chip Barker sequence [1, 1, 1, -1, -1, -1, 1, -1, -1, 1, -1] is the PN chosen for DSSS PHY layer
- Its autocorrelation shows some very sharp peaks when the transmitter and the receiver are synchronized
- The first IEEE 802.11 standard used a symbol rate of 1 Mega-symbol per second (Msps) yielding a 11 MHz chipping rate with the Barker sequence, and data rates of 1 Mbps (using DBPSK) and 2 Mbps (using DQPSK)



Peaks when correlating the sequence '10' with the 11-chip Barker sequence



Peaks when correlating a received sequence with the 11-chip Barker sequence

IEEE 802.11b and the 8-Chip Complementary Code Keying

- DSSS implemented to give data rates of 5.5 Mbps and 11 Mbps using symbol rates of 1.375 Msps (Million symbols per second) with an 8-chip Complementary Code Keying (CCK) modulation scheme
- CCK employs a nearly orthogonal complex code set called complementary sequences
- The chip rate remains consistent with the original DSSS system at 1.375 Msps · 8 chips/s = 11 Mchip/s while data rate varies to match channel conditions by changing the spreading factor and/or the modulation scheme
- The spreading length is reduced from 11 to eight chips
- This increases the symbol rate from 1 Msps to 1.375 Msps
- For the 5.5 Mbps bit rate with a 1.375 MHz symbol rate, it is necessary to transmit 4 bits/symbol (5.5 Mbps / 1.375 Mspss) and for 11 Mbps, an 8 bits/symbol

FHSS

- **FHSS PMD takes the binary bits of information from the whitened PLCP service data unit (PSDU) and transforms them into RF signals**
- ***PSDU Data Whitening***
  - **Data whitening is applied to the PSDU before transmission to minimize bias on the data if long strings of 1's or 0's appear in the PSDU**
  - **The PHY stuffs a special symbol every 4 octets of the PSDU in a PPDU frame**
  - **A 127-bit sequence generator using the polynomial $S(x) = x^7 + x^4 + 1$ and 32/33 bias-suppression encoding algorithm are used to randomize and whiten the data**
- ***Modulation***
  - **IEEE 802.11 version released in 1997 uses two-level GFSK in the FHSS PMD to transmit the PSDU at the basic rate of 1 Mbps**
  - **The PLCP preamble and PLCP header are always transmitted at 1 Mbps**
  - **Four-level GFSK is an optional modulation method defined in the standard that enables the whitened PSDU to be transmitted at a higher rate**
  - **GFSK is a modulation technique used by the FHSS PMD shifts the frequency either side of the carrier hop frequency**
  - **Four-level GFSK is similar to two-level GFSK and modulator combines two binary bits into symbol pairs (10, 11, 01, 00)**

FHSS

- Channel Hopping
  - For use in the 2.4 GHz frequency band
  - The channels are evenly spaced across the band over a span 83.5 MHz
  - Hop channels differs from country to country
  - Channel hopping is controlled by the FHSS PMD
- *IR*
  - IR PHY is one of the three PHY layers supported
  - Differs from DSSS and FHSS because IR uses near-visible light as the transmission media
  - IR communication relies on the light energy, which is by line-of-sight or reflected off objects
  - Operation is restricted to indoor environments and cannot pass through walls
- *Modulation*
  - Transmits binary data at 1 and 2 Mbps
  - Uses PPM modulation to reduce the optical power required
  - Specific data rate is dependent upon the type of PPM
  - Modulation for 1 Mbps operation is 16-PPM, while it is 4-PPM for 2 Mbps
  - PPM is a modulation technique that keeps the amplitude, pulse width constant, and varies the position of the pulse in time

FHSS

Data bits	4-PPM symbol
00	0001
01	0010
11	0100
10	1000

4-PPM symbol map for 2 Mbps

OFDM

- Standard employs 300 MHz bandwidth in the 5 GHz unlicensed national information infrastructure (UNII) band
- The spectrum is divided into three “domains,” each having restrictions on the maximum allowed output power
- The first 100 MHz in the lower frequency portion is restricted to a maximum power output of 50 mW
- The second 100 MHz has a higher 250 mW maximum
- The third 100 MHz intended for outdoor applications, has a maximum of 1.0 W power output
- OFDM in 802.11a and 802.11g combines multicarrier, multisymbol, and multirate techniques
- Divides transmitted data into multiple parallel bit streams, each with relatively lower bit rates and modulating separate narrowband carriers, referred to as sub-carriers
- The sub-carriers are orthogonal, so each can be received without interference from another
- 802.11a specifies eight non-overlapping 20 MHz channels in lower two bands; each of these are divided into 52 sub-carriers (four of which carry pilot data) of 300-kHz bandwidth each
- Four non-overlapping 20 MHz channels are specified in the upper band
- The receiver processes the 52 individual bit streams
- This multicarrier technique has some important properties such as reducing multipath and allowing individual sub-carriers to be coded accordingly
- This is also known as Coded OFDM (COFDM)
- Four modulation methods are BPSK, QPSK, 16-QAM, and 64-QAM
- 16-QAM has 16 symbols, each representing four data bits. 64-QAM has 64 symbols, each representing six data bits
- The symbol rate for a constellation is 250 Kilo symbols per second (Ksps) or the data rate for a 16-QAM is (4 bits/symbol · 250 Ksps) = 1 Mbps

IEEE 802.11a Data Rate Description

Data Rate (Mbit/s)	Modulation Type	Coding Rate (Convolution Encoding & Puncturing)	Coded bits per sub-carrier symbol	Coded bits per OFDM symbols	Data bits per OFDM symbol
6*	BPSK	½	1	48	24
9	BPSK	¾	1	48	36
12*	QPSK	½	2	96	48
18	QPSK	¾	2	96	72
24*	16-QAM	½	4	192	96
36	16-QAM	¾	4	192	144
48	64-QAM	2/3	6	288	192
54	64-QAM	¾	6	288	216

* Support for these data rates is required by the IEEE 802.11a standard

IEEE 802.11a Data Rate Description

Data Rate (Mbit/s)	Modulation Type	Coding Rate (Convolution Encoding & Puncturing)	Coded bits per sub-carrier symbol	Coded bits per OFDM symbols	Data bits per OFDM symbol
6*	BPSK	½	1	48	24
9	BPSK	¾	1	48	36
12*	QPSK	½	2	96	48
18	QPSK	¾	2	96	72
24*	16-QAM	½	4	192	96
36	16-QAM	¾	4	192	144
48	64-QAM	2/3	6	288	192
54	64-QAM	¾	6	288	216

* Support for these data rates is required by the IEEE 802.11a standard

- OFDM can eliminate inter-symbol interference at no bandwidth cost
- However, OFDM is very sensitive to frequency offsets and timing jitter

Comparison Among IEEE 802.11a/b/g

	802.11a	802.11b	802.11g
Operating frequencies	5 GHz U-NII/ISM bands	2.4 GHz ISM band	2.4 GHz ISM band
Modulation techniques	OFDM	Barker Code/CCK	Barker Code/CCK/OFDM
Data rates	6, 9, 12, 18, 24, 36, 48, 54	1, 2, 5.5, 11	1, 2, 5.5, 11 6, 9, 12, 18, 24, 36, 48, 54
Slot time	9 μs	20 μs	20 μs 9 μs (optional)
Preamble	OFDM	Long Short (optional)	Long/Short/OFDM

IEEE 802.11a/b/g

- A shorter wavelength is its main drawback
- Higher-frequency signals will have more trouble propagating through physical obstructions in an office than those at 2.4 GHz
- An advantage of 802.11a is its intrinsic ability to handle delay spread or multipath reflection effects
- The slower symbol rate and placement of significant guard time around each symbol
- Greater number of channels available to 802.11a (thirteen in US and up to nineteen in Europe) as compared to 802.11b/g
- Both 802.11b and 802.11g operate in the crowded 2.4 GHz band used by several others equipment such as Bluetooth devices, microwaves, cordless phones, garage door openers, etc.
- Drawback of backward interoperability requirement with 802.11b devices

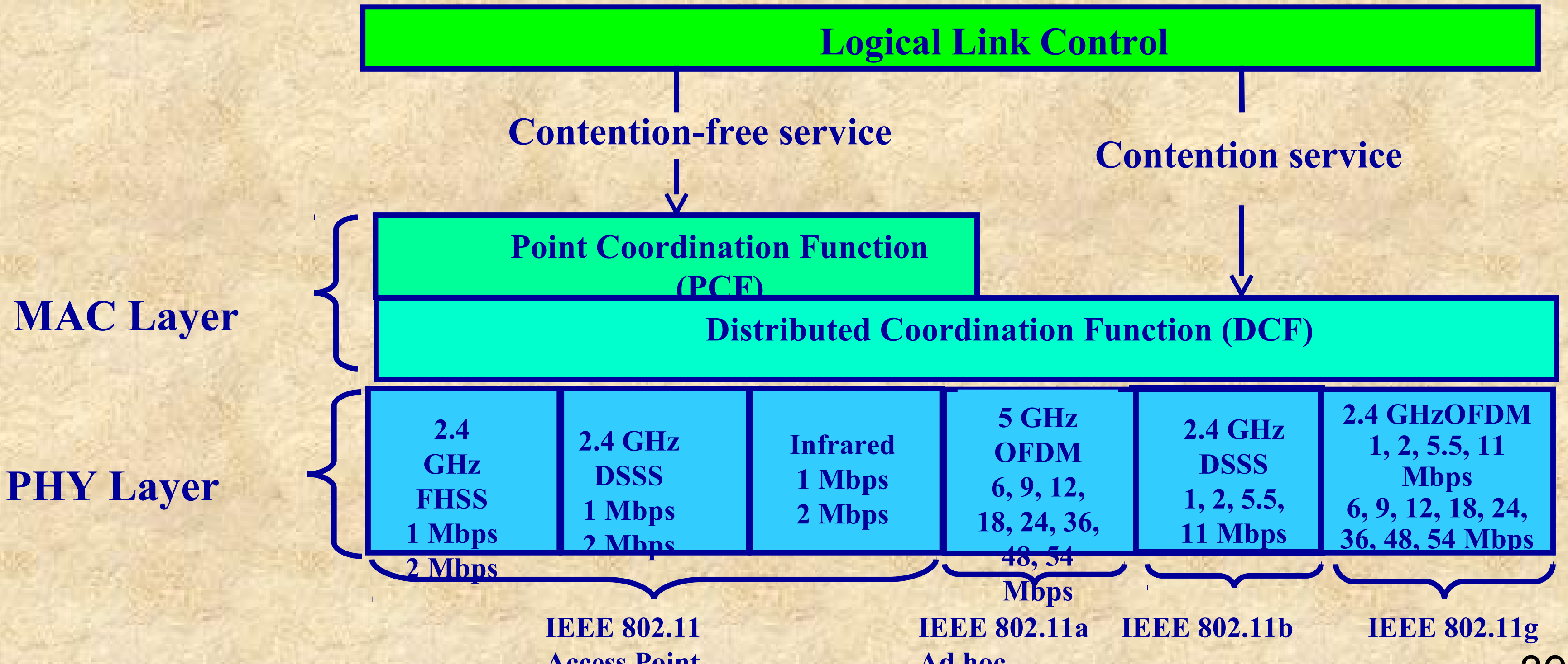
Maximum Transport Level Throughput in 802.11a/b/g

	Maximum number of non-interfering channels	Maximum link rate (Mbps)	Theoretical maximum TCP rate (Mbps)	Theoretical maximum UDP rate (Mbps)
802.11b	3	11	5.9	7.1
802.11g (with 802.11b)	3	54	14.4	19.5
802.11g Only	3	54	24.4	30.5
802.11a	19	54	24.4	30.5

- **Absence of 802.11b devices (802.11g-only environment) 802.11g throughput is equivalent to 802.11a**
- **However in a mixed mode 802.11b/g environment, 802.11g devices have to adjust some properties**
- **Worst case 802.11g performance may be as low as the slowest 802.11b device**
- **All 802.11a/b/g use dynamic rate shifting by automatically adjusting data rate based on the condition of the radio channel**

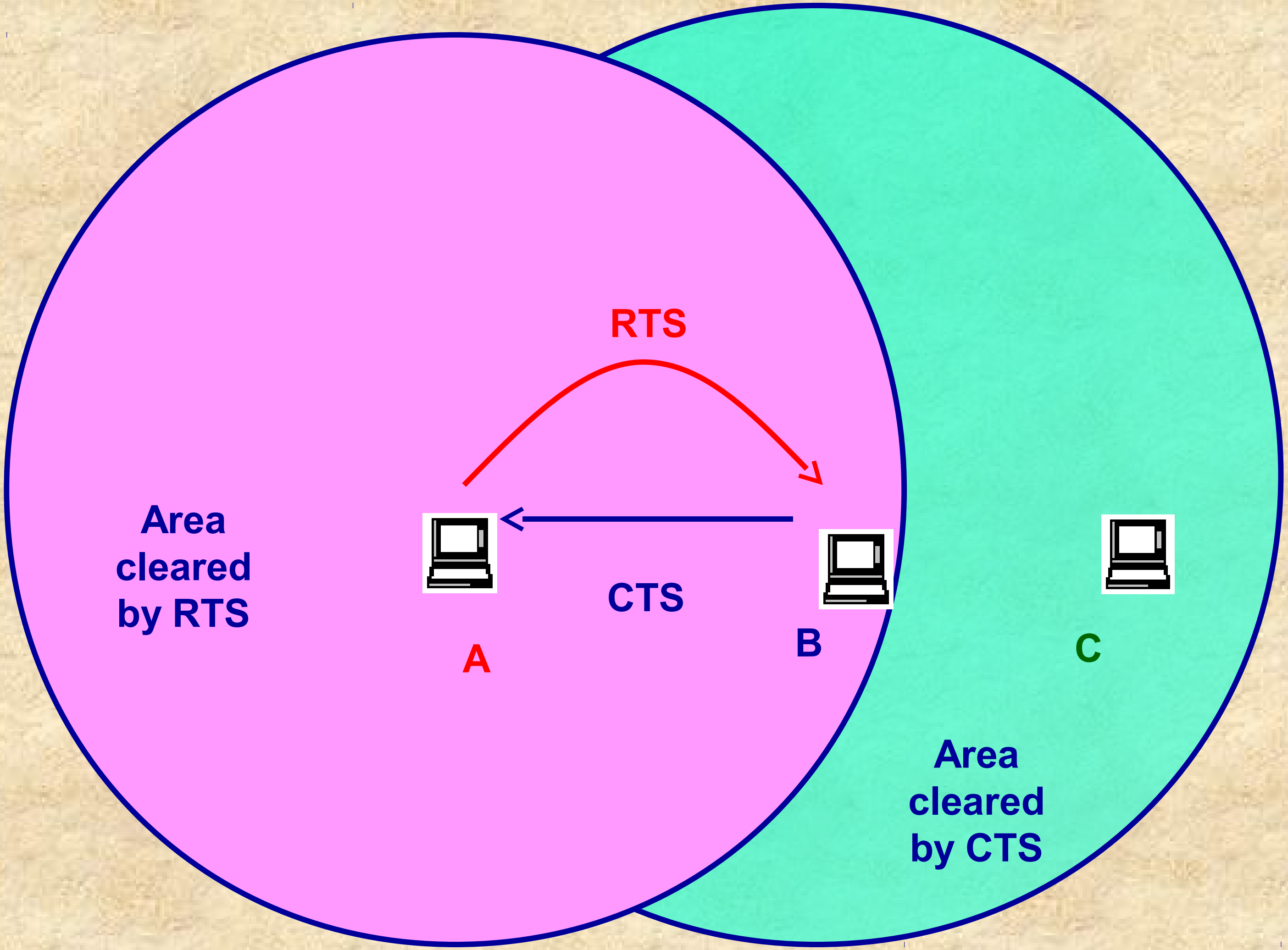
MAC Layer

- MAC protocol is the arbitration of accesses to a shared medium among several end systems
- IEEE 802.11 specifies two medium access control protocols, Point Coordination Function (PCF) and Distributed Coordination Function (DCF)
- DCF is a fully distributed scheme which enables the ad hoc networking capabilities, whereas PCF is an optional centralized scheme built on top of the basic access method



Hidden Terminal Problem

- RTS/CTS handshake
- Failure causes the RTS frame to be retransmitted
- This is treated as a collision
- Rules for scheduling the retransmission is considered later
- RTS/CTS handshake can be disabled in some situations
- Setting Network Allocation Vector (NAV)



The Retry Counters

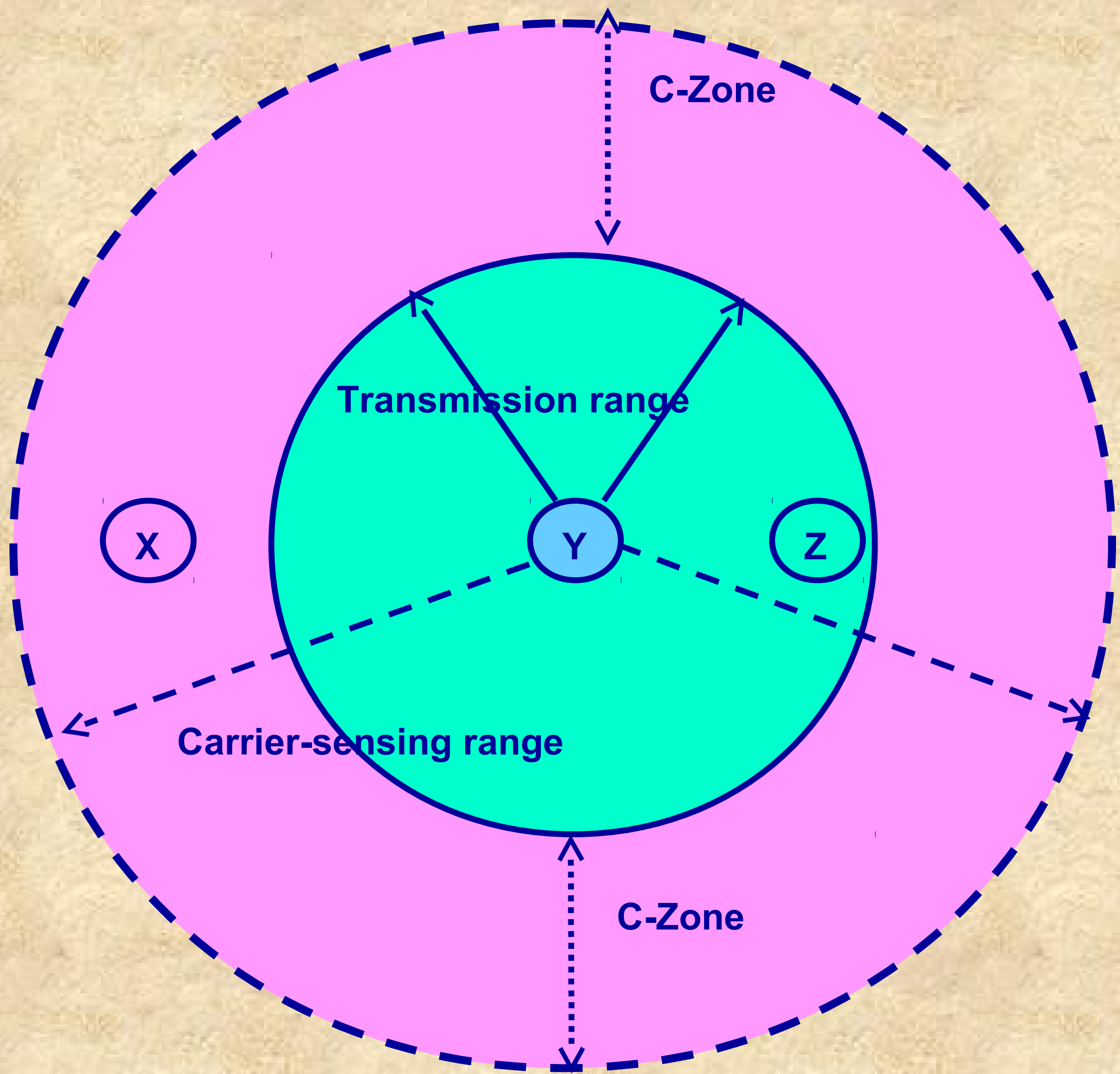
- **Two retry counters associated with MAC: A short retry counter and a long retry counter**
- **Former is associated with short frames (i.e., frames with size less than *dot11RTSThreshold*), while the latter controls long frames**
- **In addition to the counters, a lifetime timer is associated with every transmitted MAC frame**
- **Upon an unsuccessful transmission, the corresponding counters are incremented**
- **When they reach the threshold defined in the MIB (i.e., *dot11ShortRetryLimit* and *dot11LongRetryLimit*), the frame is discarded**

Time Intervals

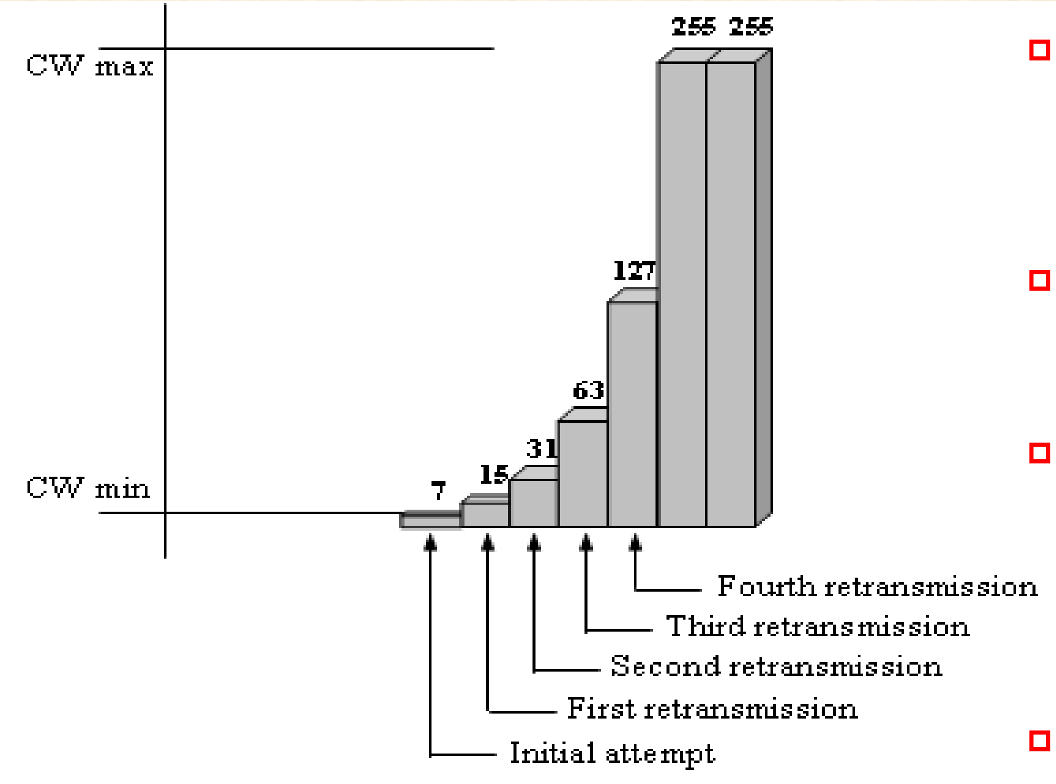
- Five time intervals
  - The slot time, defined in the PHY layer
  - The short interframe space (SIFS) defined by the PHY layer
  - The priority interframe space (PIFS)
  - The distributed interframe space (DIFS)
  - The extended interframe space (EIFS)
- Use of five time intervals
  - IFSs provide priority levels for channel access
  - SIFS is the shortest interval (equal to 10µsec), followed by the slot time which is slightly longer (equal to 20µsec)
  - PIFS is equal to SIFS plus one slot time
  - DIFS is equal to the SIFS plus two slot times
  - EIFS is much larger than any of the other intervals
  - Used by a station to set its NAV when it receives a frame containing errors, allowing the possibility for the ongoing MAC frame exchange to complete before another transmission attempt
  - These values may change from standard to standard
  - For instance, in 802.11a the slot time value has been decreased (now equal to 9µsec)

Ranges and Zones

- Transmission Range
- Carrier-sensing Range
- Interfering Range

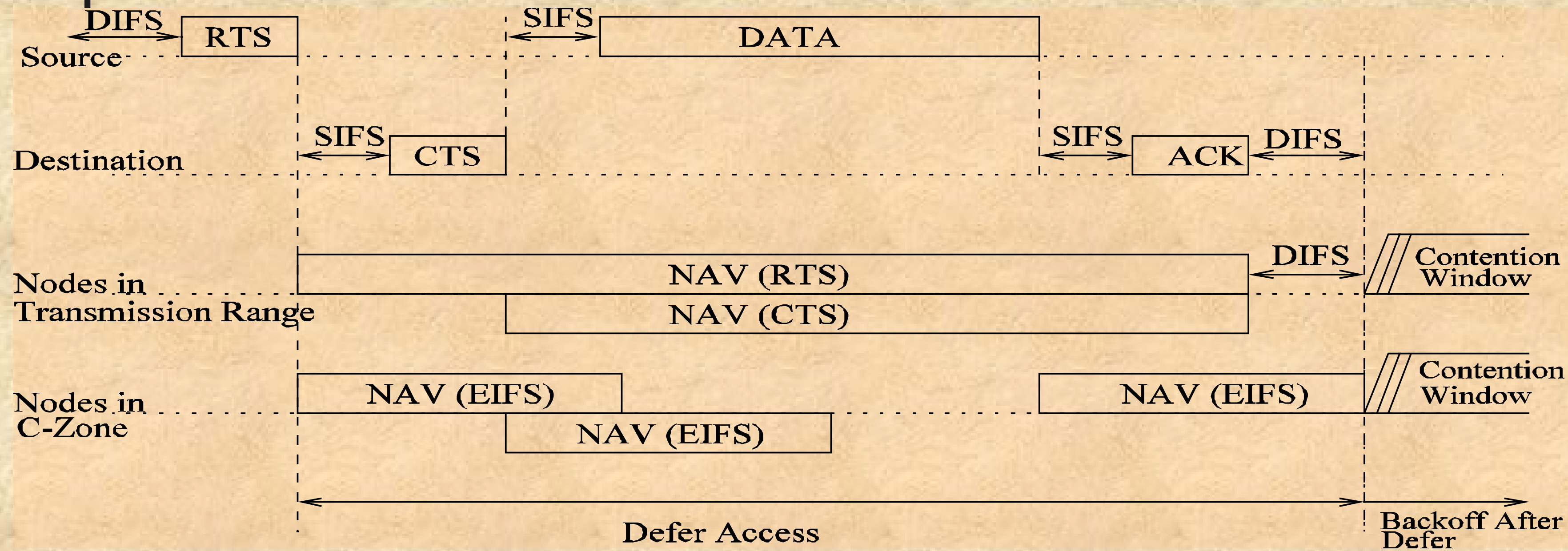


Distributed Coordination Function (DCF)



- Two forms of carrier sensing: physical (by listening to the wireless shared medium) and virtual
- Virtual carrier sensing uses the duration field to set a station's NAV which is included in the header of RTS and CTS frames
- If medium found idle for more than a DIFS period, then the frame can be transmitted
- Otherwise, the transmission is deferred and the station uses an Exponential Random Backoff Mechanism by choosing a random backoff interval from [0, CW]
- If collision occurs, the station doubles its CW
- At the first transmission attempt, CW = CWmin and is doubled at each retransmission up to CWmax

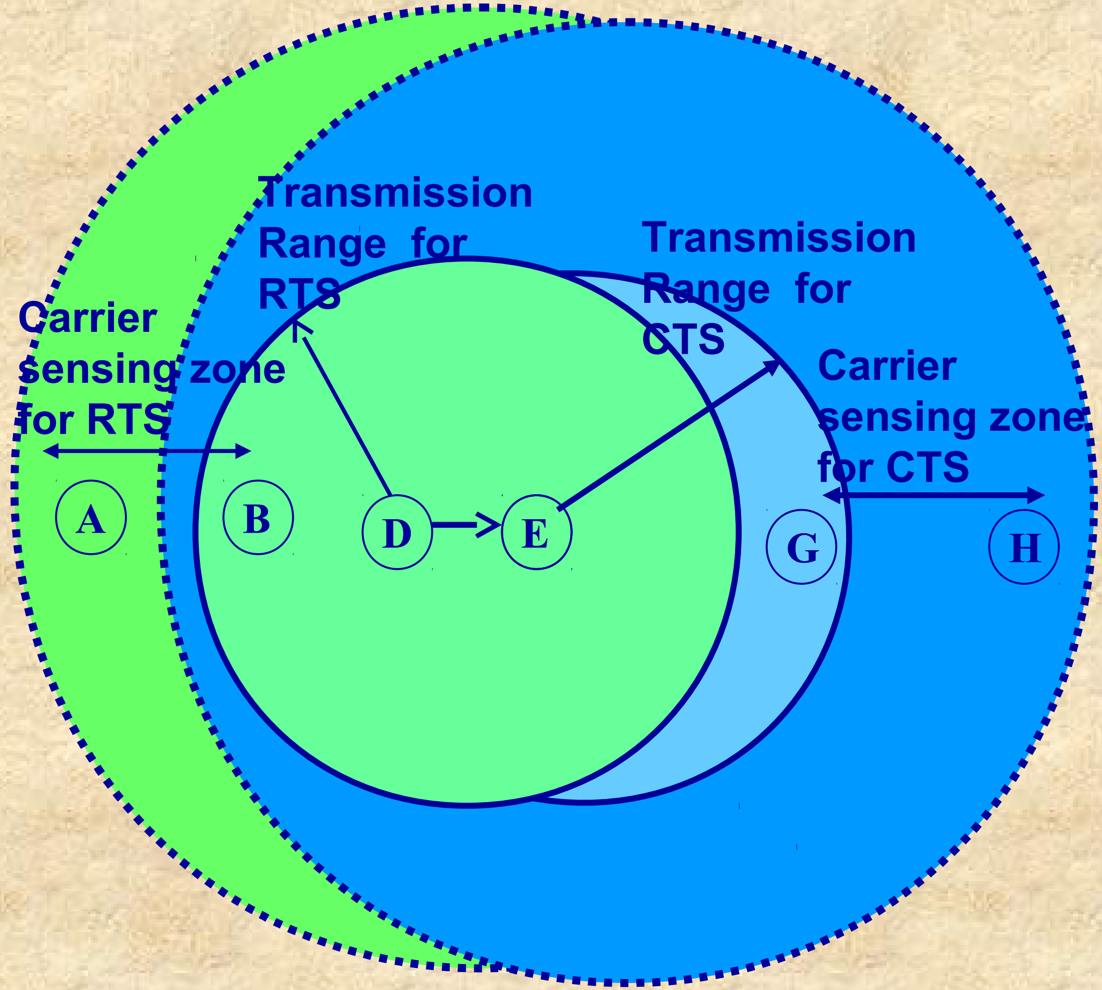
802.11 with RTS/CTS



- Basic access mechanism of IEEE 802.11 can be extended by the RTS/CTS frame exchange to reserve channel before data transmission
- When a station wants to send a frame larger than above a specified threshold (*dot11RTSThreshold*), it first sends a short control frame RTS to the destination station
- The destination then sends, after a SIFS, another short control frame CTS back to the source
- The source then transmits its DATA frame after SIFS period as the channel is reserved for itself during all the frame duration
- Both RTS and CTS frames carry the duration needed
- After the destination receives the DATA, it sends an ACK back to the source after SIFS period

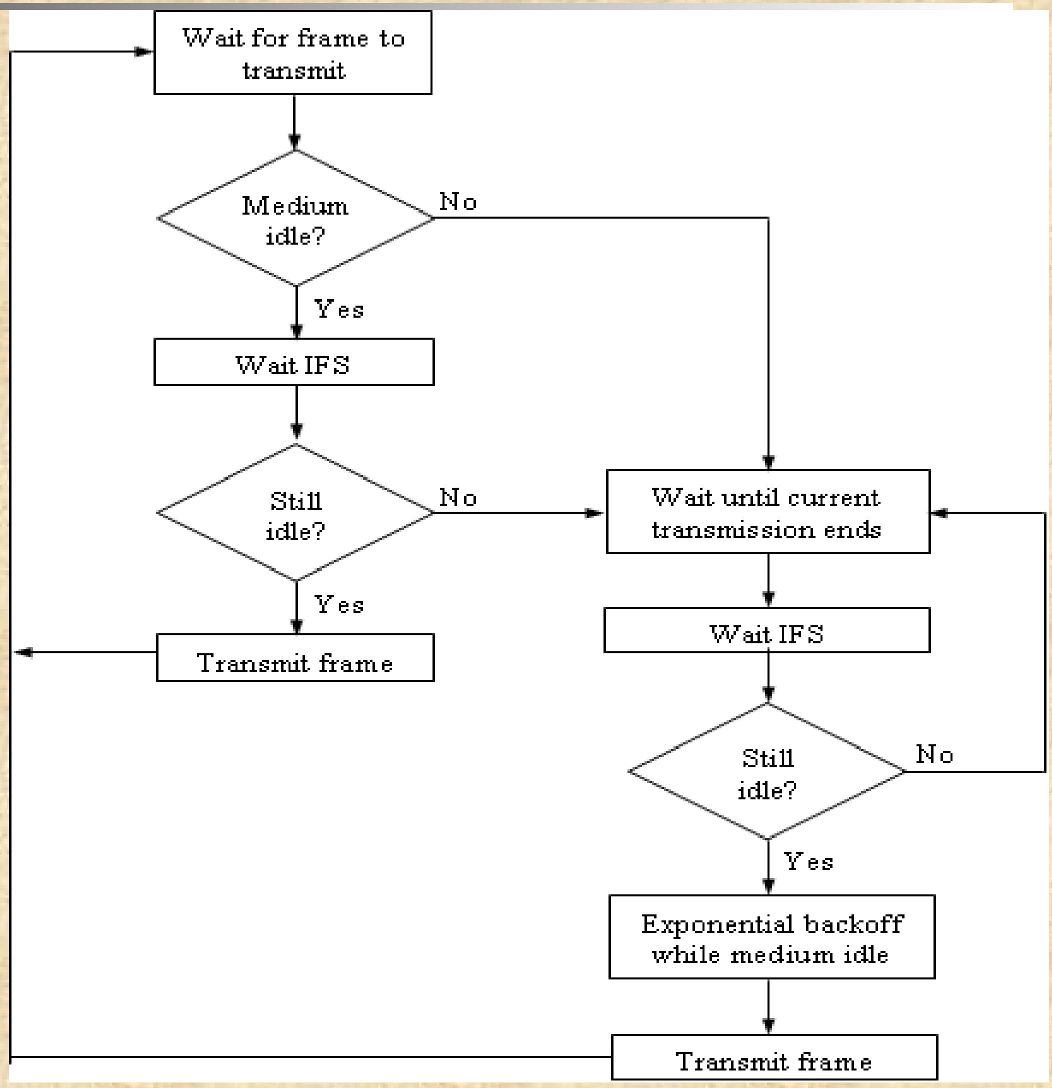
Collisions not completely avoided in IEEE 802.11

- Nodes in transmission range correctly set their NAVs when receiving RTS or CTS
- However, since nodes in the C-zone cannot decode the packet, they do not know duration
- To prevent a collision with the ACK reception, nodes within the C-zone set their NAVs for the EIFS duration
- IEEE 802.11 does not completely prevent collisions due to a hidden terminal
- Nodes in the receiver's C-zone but not in the sender's C-zone or transmission range, can cause a collision with the reception of a DATA packet at the receiver



Point Coordination Function (PCF)

- PCF employs a poll and response protocol so as to eliminate the possibility of contention for the medium
- A point coordinator (PC) controls the medium access and is often co-located with the AP
- PC maintains a polling list, and regularly polls the stations for traffic while also delivering traffic to the stations
- PCF is built over the DCF, and both of them operate simultaneously
- PC begins a period of operation called the contention-free period (CFP)
- CFP occurs periodically to provide a near-isochronous service to the station
- CFP begins when the PC gains access to the medium, by using the normal DCF procedures
- During the CFP, the PC ensures that the interval between transmissions to be no longer than PIFS



The MAC control logic

Framing

- MAC layer accepts MAC Service Data Units (MSDUs) from higher layers and adds appropriate headers and trailers to create MAC Protocol Data Units (MPDU)
- MAC may fragment MSDUs into several frames, hence attempting to increase the probability of each individual frame being delivered successfully
- Header + MSDU + Trailer contain the following information:
  - Addressing information
  - IEEE 802.11-specific protocol information
  - Information for setting the NAV
  - Frame check sequence for integrity verification

General Frame Format

Bytes:

Frame Control	Duration ID	Addr 1	Addr 2	Addr 3	Sequence Control	Addr 4	Frame body	CRC
2	2	6	6	6	2	6	0-2312	4

← IEEE 802.11 MAC Header →

The IEEE 802.11 MAC frame format

Bits:

Protocol Version	Type	Subtype	To DS	From DS	More Flag	Retry	Pwr Mgt	More Data	WEP	Ord
2	2	4	1	1	1	1	1	1	1	1

The Frame Control field

Frame Control (FC)

- Frame Control field is composed of a total of eleven sub-fields which adds up to a total of 2 bytes and are:
  - Protocol Version
  - Frame Type and Sub Type
  - *To DS* (Distribution System) and *From DS*
  - More Fragments
  - Retry
  - Power Management
  - More Data
  - WEP (Wired Equivalent Privacy)
  - Order
- Duration ID (D/ID)
  - D/ID contains information for setting the NAV by setting 15th bit to zero
- Address Fields: Four
  - The IEEE 48-bit address comprises of three fields
  - A single-bit Universal/Local bit
  - BSS Identifier (BSSID)
  - Transmitter Address (TA)
  - Source Address (SA)
  - Destination Address (DA)

Frame Control (FC)

- *Sequence Control*
  - 4-bit fragment number and a 12-bit sequence number
  - Fragment Number sub-field
  - Sequence Number sub-field
- *Frame Body*
  - A variable length field which contains the information specific to the particular data or management frame.
  - It can go up to 2304 bytes, and 2312 bytes when encrypted
- *Frame Check Sequence (FCS)*
  - An IEEE 802 standard generated similar to IEEE 802.3, using the following CRC-32 polynomial:

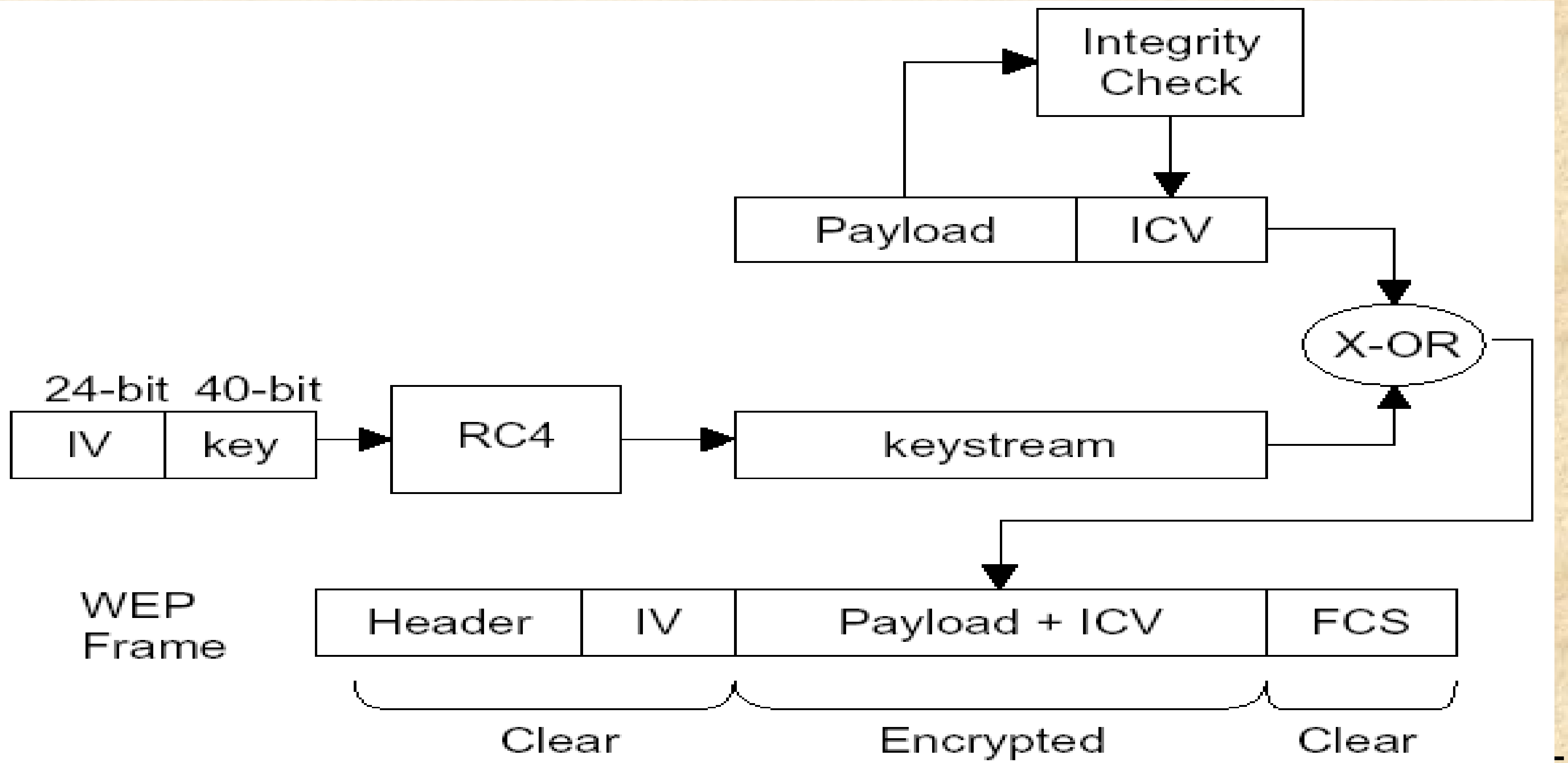
$$G(x) = x^{32} + x^{26} + x^{23} + x^{22} + x^{16} + x^{12} + x^{11} + x^{10} + x^{8} + x^{7} + x^{5} + x^{4} + x^{2} + x + 1$$

Control Frame Subtypes

- ***Request To Send (RTS)***
  - **This is a 20 bytes frame which includes the FC field, the Duration field, the RA and the TA fields, and the FCS**
- ***Clear To Send (CTS)***
  - **This is a 14 bytes frame which contains the FC field, the Duration field, the RA, and the FCS field**
- ***Acknowledgement (ACK)***
  - **FC Field**
  - **Duration/ID Field (ms)**
  - **RA**
  - **FCS**
- ***Data Frame Subtypes***
  - **Data frame is variable in length (from 29 to 2346 bytes)**
  - **Address 2 field is used to identify the sender of the frame**
  - **Address 3 field carries additional information for frame filtering or forwarding by the DS**
  - **Address 4 field is used only in a wireless DS as one AP forwards a frame to another AP**
  - **DA is the destination of the MSDU in the frame body field**
  - **SA is the address of the MAC entity that initiated the MSDU in the frame body field**
  - **RA is the address of the station contained in the AP in the wireless DS that is next recipient**
  - **TA is the address of the station contained in the AP in the wireless DS that is transmitting the frame**
  - **BSSID is the address currently in use by the station contained in the AP if the station is the AP or is associated with an AP**

WEP Security Mechanisms

- WEP security mechanisms include data encryption and integrity
- To prepare a protected frame, first an integrity check value (ICV) of the frame payload is computed using a cyclic redundancy check (CRC) function
- The cleartext payload concatenated with the ICV is then encrypted using a bit-wise Exclusive-OR operation with a pseudorandom keystream



WEP Security Flaws

- Suffers from many design flaws
- Data encryption based on an approximation of the "one-time pad" algorithm
- Like WEP encryption, one-time pad encryption consists of the bit-wise Exclusive-OR between a binary plaintext message and a binary keystream
- The secrecy of the resulting cipher text is perfect, provided that each new message is encrypted with a different secret random keystream
- The secrecy is not guaranteed when the keystream is re-used or its values can be predicted
- Hence, a first class of attacks on WEP exploits possible weaknesses in WEP's keystream generation process that makes the secret keystream easily predictable or causes its re-use

The IEEE 802.11i Amendment: A New Security Scheme

- Amendment called 802.11i. IEEE 802.11i, also known as Wi-fi Protected Access (WPA)
- Three major parts: Temporal Key Integrity Protocol (TKIP), counter mode cipher block chaining with message authentication codes (counter mode CBC-MAC) and IEEE 802.11x access control
  - TKIP fixes its well-known problems, including small IV and short encryption keys
  - Counter mode CBC-MAC is designed to provide link layer data confidentiality and integrity
  - Centralized, server-based authentication occurs when a client first joins a network and then, authentication periodically recurs to verify the client has not been subverted or spoofed
- System Design Considerations
  - The Medium
  - *Multipath*
  - Path Loss

Delay spread for various environments

Environment	Delay Spread
Home	~50 nsec
Office	~100 nsec
Manufacturing floor	200-300 nsec

Multipath Fading and 802.11's

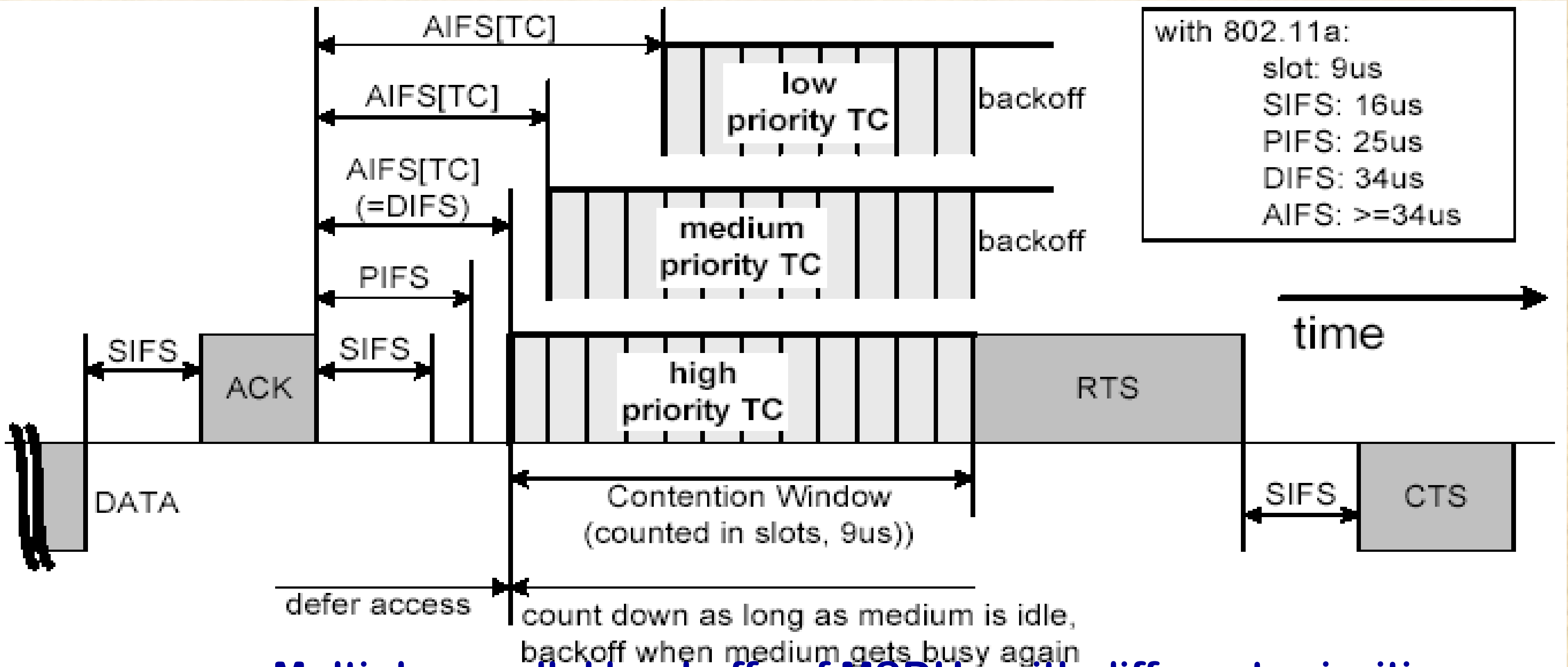
- Es/No vs. BER (Bit-Error-Rate) Performance
- Interference in the 2.4 GHz ISM Band
- An Overview of Past and Present IEEE 802.11 Efforts
  - 802.11a: in the 5 GHz radio band, with thirteen available radio channels, with the maximum link rate per channel is of 54 Mbps
  - 802.11b: in the 2.4 GHz radio band with the maximum link rate per channel is of 11 Mbps
  - 802.11d : this standard cannot legally operate in some countries, and the purpose of 802.11d is to add features and restrictions to allow WLANs to operate within the rules of those countries
  - 802.11e: is supplementary to the MAC layer to provide QoS support for 802.11 physical standards a, b and g
  - 802.11f: is a recommended practice document that enables interoperability between a multi-vendor WLAN networks
  - 802.11g: physical layer standard in the 2.4 GHz and 5 GHz radio bands and specifies three non-overlapping radio channels similar to 802.11b, with a maximum link rate is 54 Mbps per channel using OFDM modulation but, for backward compatibility with 802.11
  - 802.11h: supplementary to the MAC layer so as to comply with European regulations for 5 GHz WLANs with transmission power control (TPC) and dynamic frequency selection (DFS)
  - 802.11i: a part of a set of security features that should address and overcome security issues and applies to 802.11 physical standards a, b and g
  - 802.11j: to enhance the 802.11 standard and amendments enabled addition of channel selection for 4.9 GHz and 5 GHz in Japan

Multipath Fading

- An Overview of Past and Present IEEE 802.11 Efforts
  - *802.11k: to define Radio Resource Measurement enhancements that provide mechanisms to higher layers for radio and network measurements*
  - *802.11n:* to develop enhancements for higher throughput that allows consumers and businesses to transmit data at rates greater than 100 Mbps
  - *802.11p:* expands wireless networking useful to automobiles
  - *802.11r:* task group is working on speeding up the data signal transfer speed, also known as handoff, between wireless access points
  - *802.11s:* task group is working on a new standard to support extended set of service for mesh networks which can be seen as an ad hoc network with massive increment in bandwidth and reliability
  - *802.11t:* to define a recommended practice for the evaluation of 802.11 wireless performance, which is currently done on an ad hoc basis
  - *802.11u:* 802.11 hotspot deployment has experienced tremendous growth throughout the world, the task group is developing a standard specifying how 802.11 networks can work with other external networks
  - *802.11v:* to develop an amendment to both the IEEE 802.11 PHY and MAC that provides wireless network management of client stations
  - *802.11w:* to develop enhancements to the IEEE 802.11 MAC that enable data integrity, data origin authenticity, replay protection, and data confidentiality for selected IEEE 802.11 *management* frames
  - *802.11x:* for regulating access control for stations to a network via the use of extensible authentication methods applicable to 802.11 physical standards a, b and g

The IEEE 802.11e MAC Protocol

- To effectively support QoS, the 802.11e MAC defines the Hybrid Coordination Function (HCF) that replaces DCF and PCF modes in IEEE 802.11 standard
- Two parts: the Extended Distributed Channel Access (EDCA) and the HCF Controlled Channel Access (HCCA)
- MSDUs are now delivered through multiple backoff instances within one station, wherein each backoff instance parameterized with Traffic Categories-specific parameters



Multiple parallel backoffs of MSDUs with different priorities

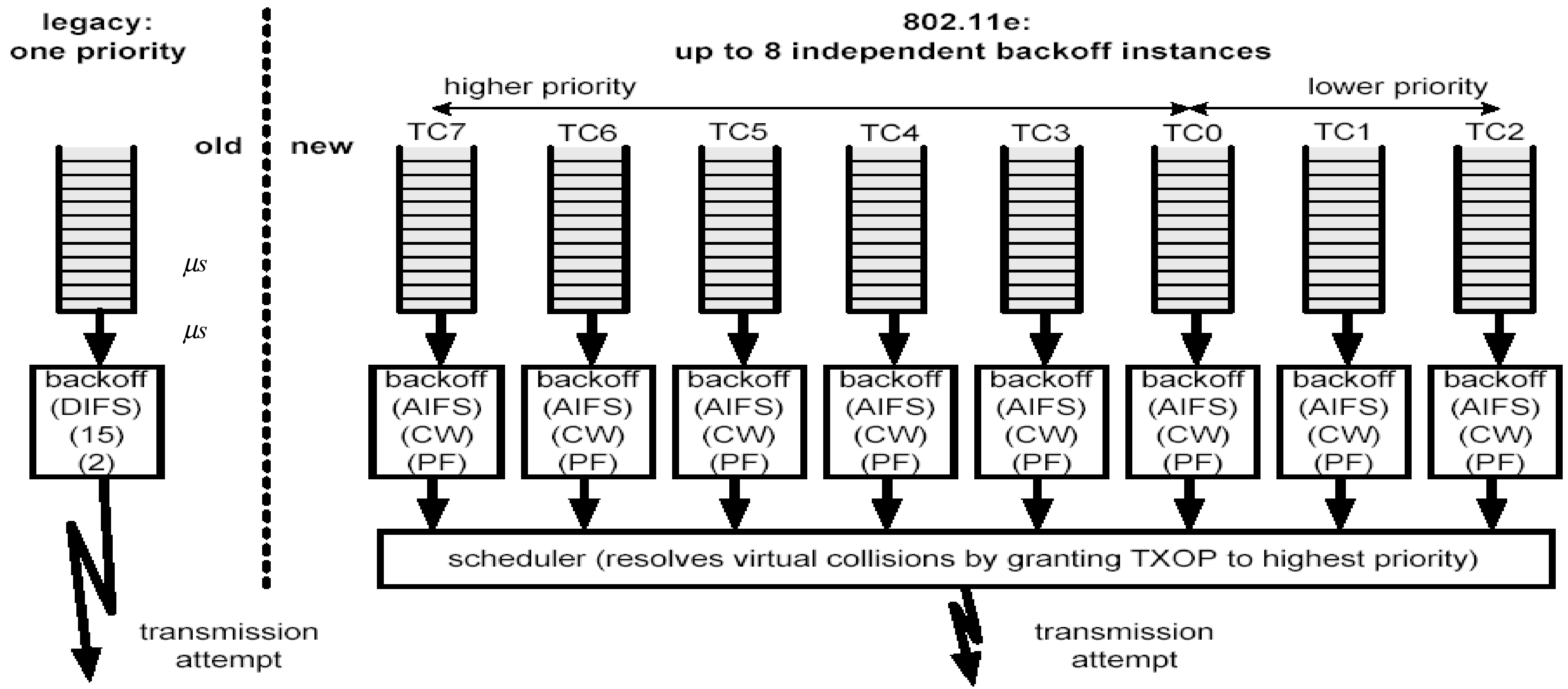
The IEEE 802.11e MAC Protocol

- Each backoff sets a counter to a random number drawn from the interval [1;CW+1]
- When the medium is determined busy before the counter reaches zero, the backoff has to wait for the medium being idle for AIFS again, before resuming the count down process
- When the medium is determined as being idle for the period of AIFS, the backoff counter is reduced by one beginning the last slot interval of the AIFS period
- After any unsuccessful transmission attempt, a new CW is calculated with the help of the persistence factor (PF), PF[TC], and another uniformly distributed backoff counter out of this new, enlarged CW is drawn, so that the probability of a new collision is reduced
- PF to increase the CW differently for each TC and is given by:

$$newCW[TC] \geq ((oldCW[TC]+1)\cdot PF)-1$$

- CW never exceeds the parameter CWmax[TC]
- A single station may implement up to eight transmission queues realized as virtual stations inside a station, with QoS parameters that determine their priorities
- If the counters of two or more parallel TCs in a single station reach zero at the same time, a scheduler within the station avoids the virtual collision
- There is still a possibility that a transmitted frame could collide at the wireless medium with a frame transmitted by other stations
- Another important part is the *TXOP* which is an interval of time when a station has the right to initiate transmissions, defined by a starting time and a maximum duration

Virtual back of eight traffic categories



Virtual back of eight traffic categories

(1) Left: legacy DCF close to EDCA with AIFS=34, C W min=15, PF=2;

(2) Right: EDCA with AIFS[TC] ≥ 34, C W min [TC]=0-255, PF[TC]=1-16

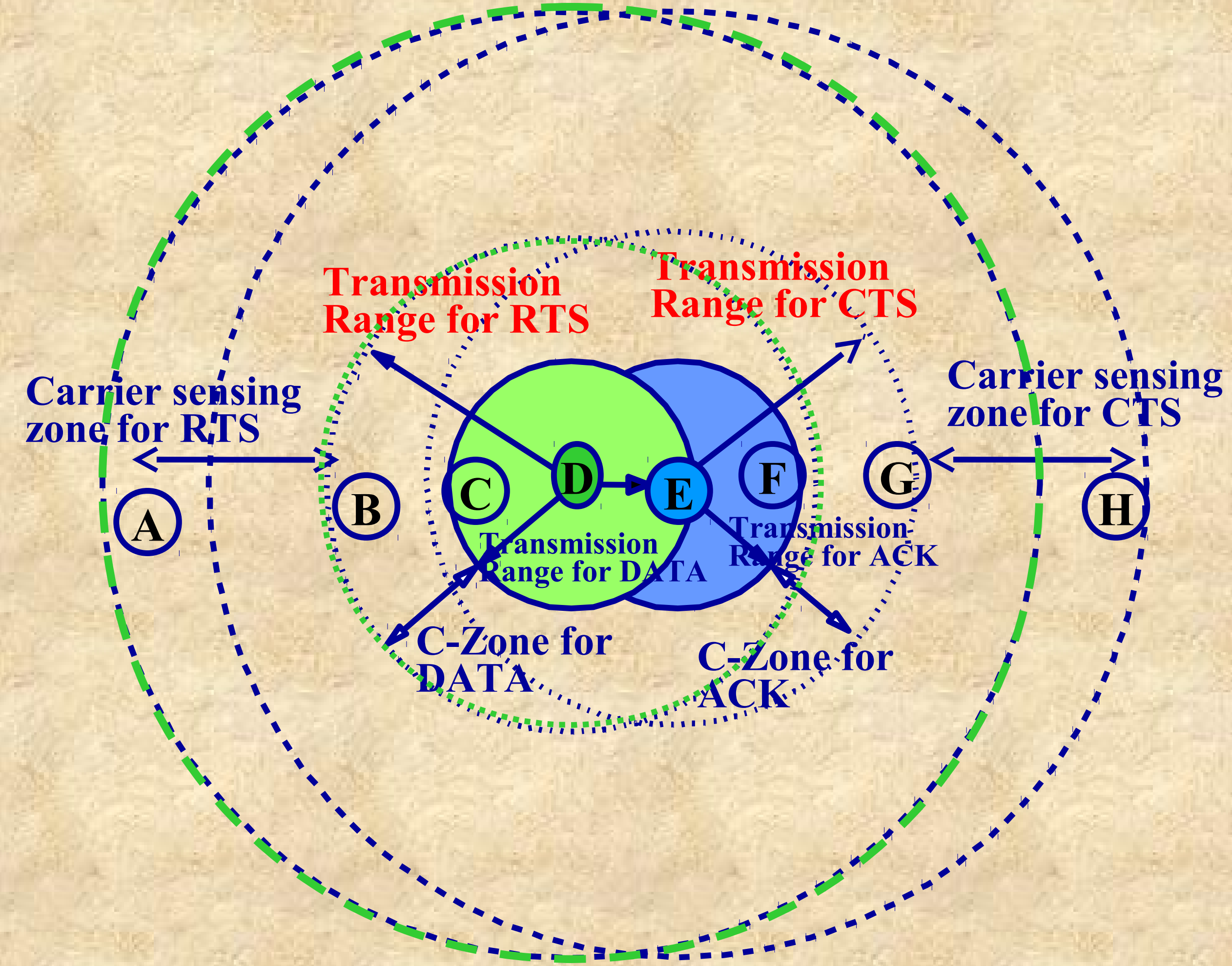
The HCCA

- The HCCA extends the EDCA access rules by allocating TXOPs to itself in order to initiate MSDU Deliveries whenever it desires, however, only after detecting the channel as being idle for PIFS
- To give the HC priority over the EDCA, AIFS must be longer than PIFS and can therefore not have a value smaller than DIFS
- The QoS CF-Poll from the HC can be sent after a PIFS idle period without any backoff
- An additional random access protocol that allows fast collision resolution is defined
- The controlled contention mechanism allows stations to request the allocation of polled TXOPs by sending resource requests, without contending with other EDCA traffic
- This control frame forces legacy stations to set their NAV until the end of the controlled contention interval, thereby remaining silent during the controlled contention interval

Enhancements to IEEE 802.11 MAC

- Power Control
  - Power control can also increase effective capacity of the network by enhancing spatial reuse of the wireless channel
  - Current research on power control MAC protocols focus on suitably varying transmit power in order to reduce energy consumption
  - May be classified based upon the presence or absence of asymmetric links between nodes
- The BASIC Protocol
  - Power control can can also lead to asymmetry between nodes
  - This asymmetry is addressed by transmitting the RTS and CTS packets at maximum possible power level (p_{max}), while transmitting DATA and ACK at lowest power level needed to communicate ($p_{desired}$)
  - In the BASIC scheme, when nodes receive either a RTS or CTS packet (always transmitted at p_{max}), they set their NAVs for the duration of the DATA and ACK transmission
  - In regular IEEE 802.11, the C-zone is the same for RTS-CTS and DATA-ACK since all packets are sent using the same power level (p_{max})
  - In the BASIC scheme, the transmission range for DATA-ACK is smaller than that of RTS-CTS whenever a source and destination pair decides to reduce the transmit power for DATA-ACK
  - Similarly, the C-zone for DATA-ACK is also smaller than that of RTS-CTS

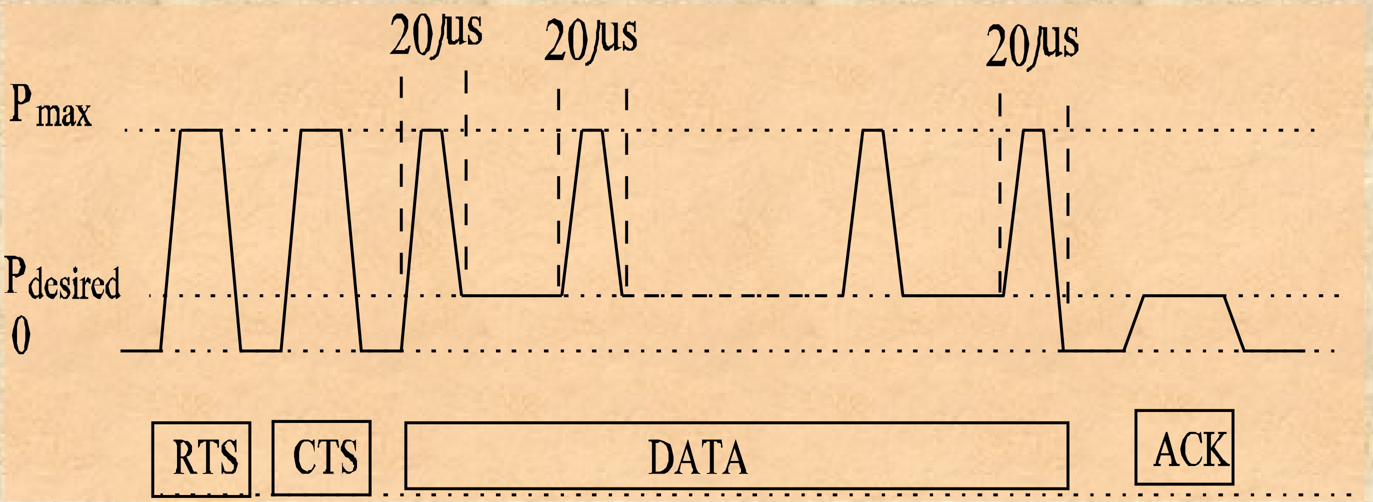
The BASIC Protocol



The BASIC protocol

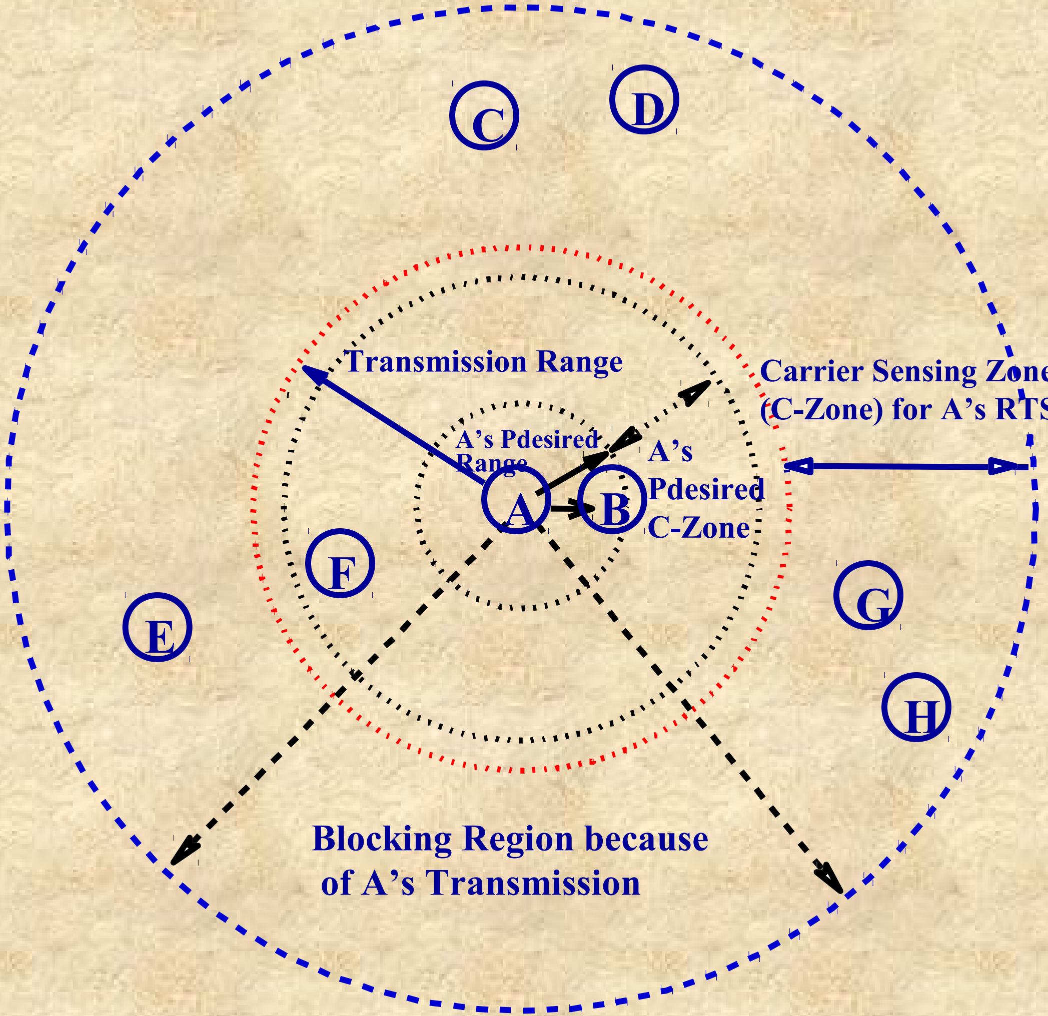
The Power Control MAC Protocol

- To address the deficiency of the BASIC protocol, the PCM protocol has been proposed
- Similar to the BASIC protocol, PCM transmits the RTS and the CTS packets at p_{max} and use the minimum power level (that is, $p_{desired}$) needed for communication for DATA and ACK
- However, contrary to the BASIC scheme, eventual collisions with nodes in the C-zone are avoided by making the source node in a transmission periodically transmit the DATA packet at p_{max} so that nodes in the C-zone can sense the signal and set their NAVs accordingly
- Transmit power level transitions in PCM during a regular sequence of RTS-CTS-DATA-ACK transmission shown below



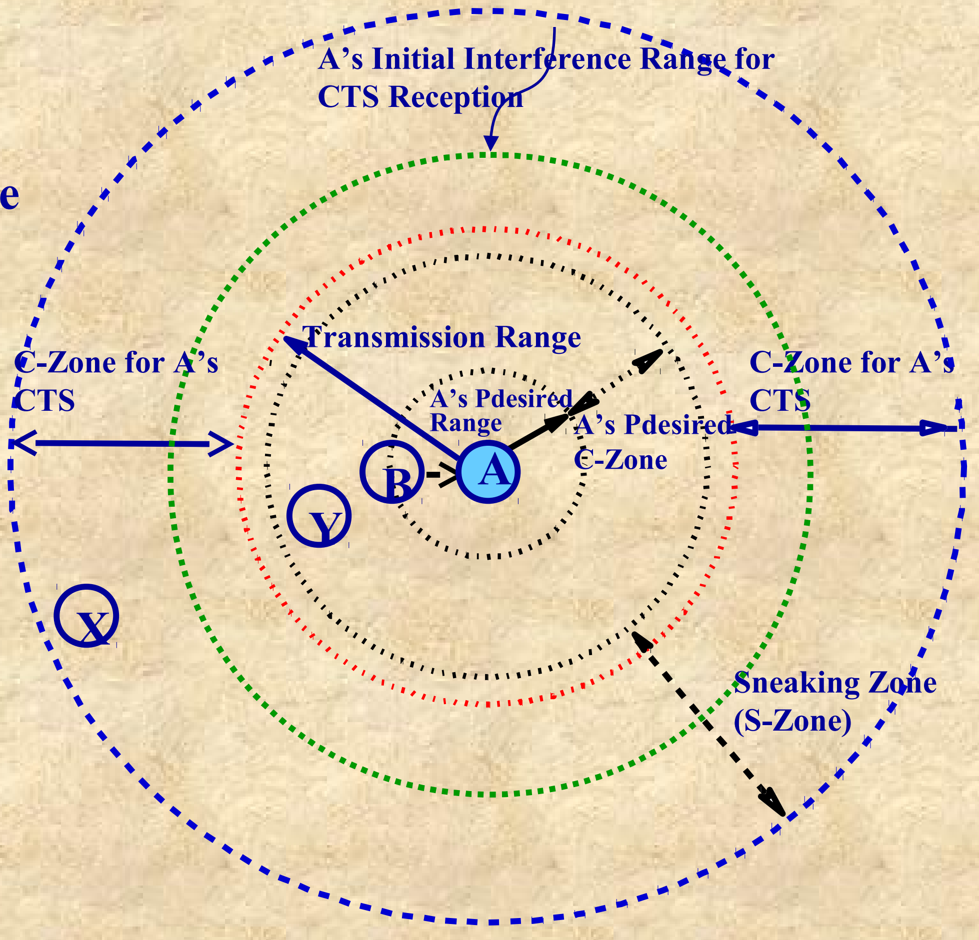
Power Control in PCM

- PCM overcomes the deficiency of the BASIC scheme and can achieve throughput comparable to that of IEEE 802.11 with less energy consumption
- However, note that PCM, just like 802.11, does not prevent collisions completely
- Despite of all this, PCM suffers from a drawback, namely, the inability to achieve spatial reuse
- Note that this shortcoming is also present in other existing power control MAC protocols



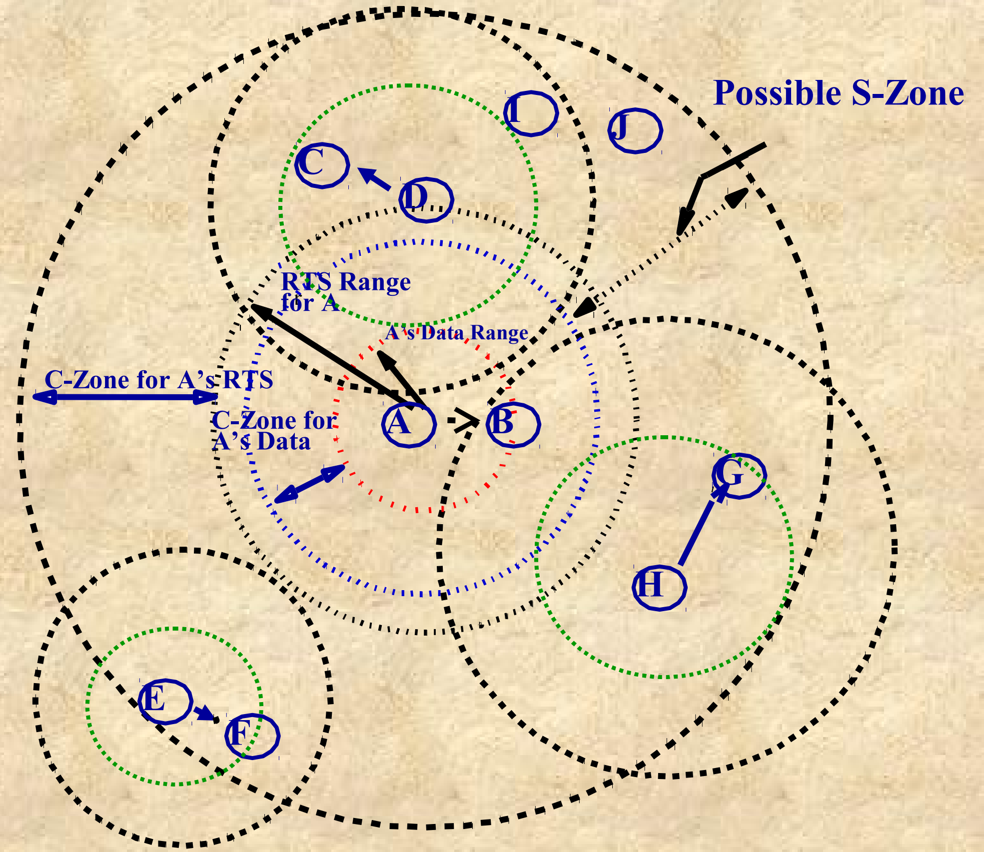
Spatial Reusability

- Spatial Reuse MAC (SRM) protocol is introduced which uses power control and employs a distributed form of transmission sneaking to accomplish appropriate spatial reuse of the channel
- The SRM protocol is similar to the BASIC scheme in that it transmits RTS and CTS at P_{max}, and DATA and ACK at $P_{desired}$
- However, SRM implements a fully distributed *transmission sneaking technique* so as to enable channel spatial reuse
- Transmission sneaking is a spatial reuse by which a pair of nodes can communicate despite the ongoing transmission in its radio range (explained in the next slide)



Channel Spatial Reusability

- The size of the S-Zone may be larger than the C-Zone
- It may also include a part of RTS-CTS transmission range, which becomes free because of the low power DATA-ACK transmission
- This reduces the carrier-sensing range of the communication between A and B
- SRM differentiates between two types of transmission:
  - *Dominating Transmission*
  - *Sneaking Transmission*

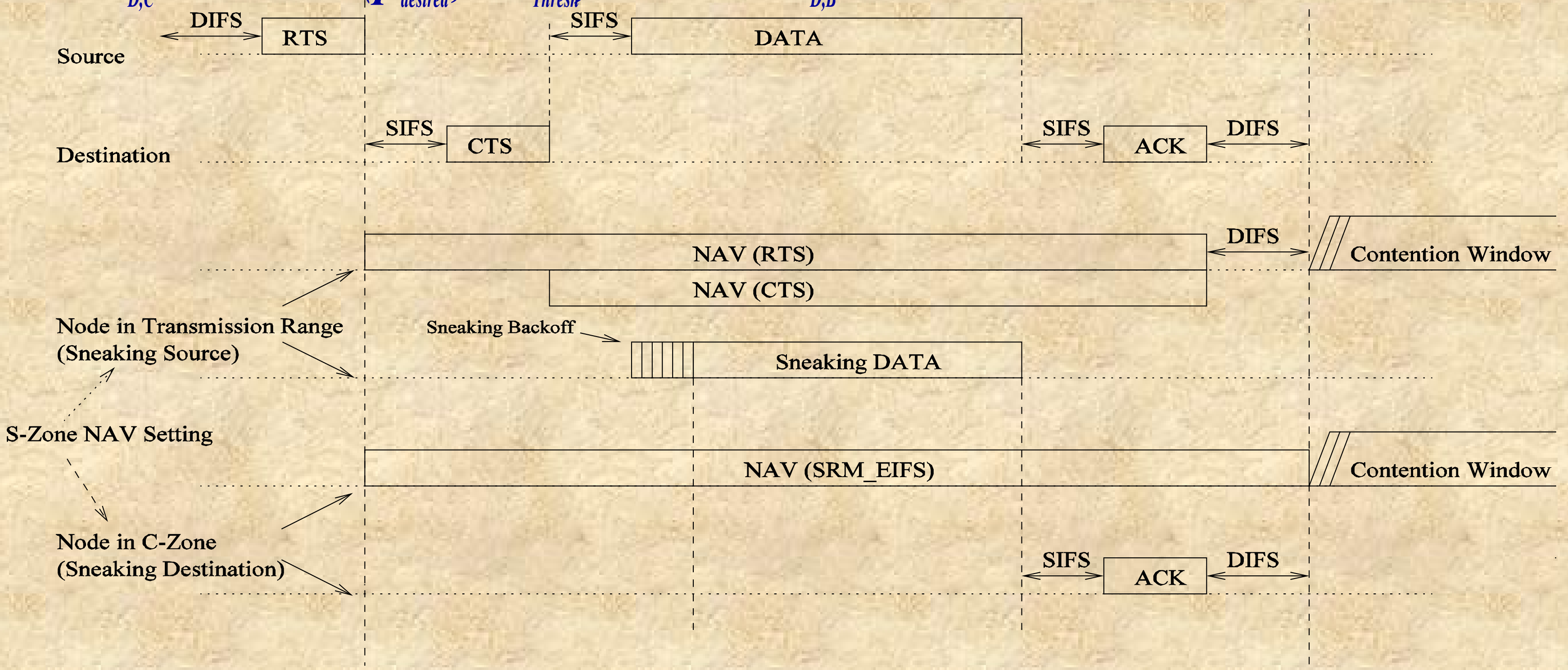


Channel spatial reusability in the SRM protocol

Mathematically speaking, node D, can sneak a packet at $p_{desired}$ to node C during the DT between nodes A and B if:

$distance_{D,C} + distance(p_{desired}, CS_{Thresh}) < distance_{D,A}$ **; and**

$distance_{D,C} + distance(p_{desired}, CS_{Thresh}) < distance_{D,B}$



QoS Provisioning

- An Extension to the IEEE 802.11 DCF
  - A scheme to extend the IEEE 802.11 DCF with the ability to support at least two service classes: premium service (i.e., high priority) and best-effort
  - Traffic of premium service class is given lower values for congestion window than those of best-effort traffic
  - If packets of both types collide, the packet with smaller congestion window value is more likely to access the medium earlier
- The Black Burst Contention Scheme
  - Avoids packet collision in a very distinctive way, while at the same time solving the packet starvation problem
  - Packets from two or more flows of the same service class are scheduled in a distributed manner with fairness guarantees
  - Nodes with best-effort traffic and nodes with real-time traffic use different interframe space values to provide higher priority
  - Each contending node is using a BB with different length, where the length of each BB is an integral number of black slots
- The MACA/PR Protocol
  - Multi-hop Access Collision Avoidance with Piggyback Reservation (MACA/PR) protocol provides guaranteed bandwidth support (via reservation) for real-time traffic
  - The first data packet in the real-time stream makes reservations along the path
  - A RTS/CTS handshake is used on each link for this first packet in order to make sure that it is transmitted successfully
  - When the sender transmits the data packet, it schedules the next transmission time after the current data transmission and piggybacks the reservation in the current data packet

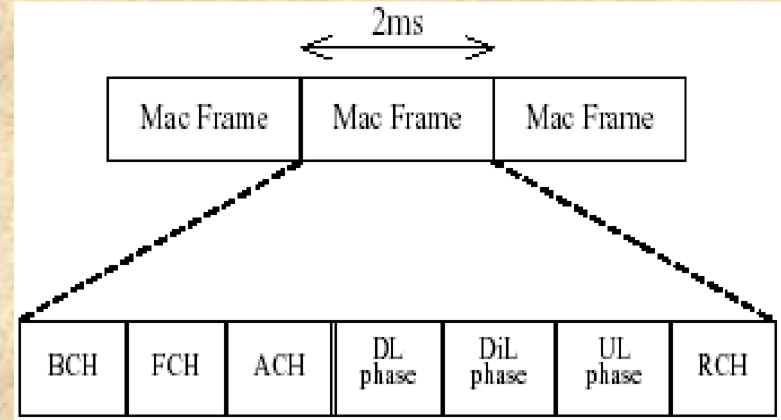
The HIPERLAN/2 Standard for Wireless LANs

- HIPERLAN/2 standard also operates at 5 GHz frequency band similarly to 802.11a
- HIPERLAN/2 and 802.11 standards primarily differ in the MAC layer, however some minor differences are also present in the PHY layers
- HIPERLAN/2 radio network is defined in such a way that there are core-independent PHY and data link control (DLC) layers as well as a set of convergence layers (CLs) for internetworking
- The CLs include Ethernet, ATM, and IEEE 1394 infrastructure and technical specifications for HIPERLAN/2–third generation (3G) internetworking have also been completed
- Physical Layer
  - OFDM is used to combat frequency selective fading and to randomize the burst errors caused by a wideband fading channel
  - Exact mechanism for different coding and modulation schemes is not specified in the standards
  - Data for transmission is supplied to the PHY layer in the form of an input PDU train or PPDU frame
  - This is then input to a scrambler that prevents long runs of 1s and 0s in the input data being sent to the remainder of the modulation process
  - Although both 802.11a and HIPERLAN/2 scramble the data with a length 127 pseudorandom sequence, the initialization of the scrambler is different
  - The coded data is interleaved in order to prevent error bursts
  - In order to prevent ISI and intercarrier interference (ICI) due to delay spread, a guard interval is implemented by means of a cyclic extension

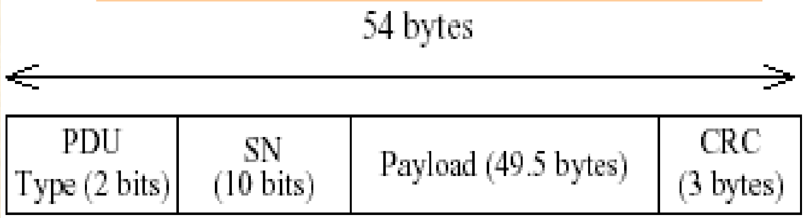
MAC Layer for HIPERLAN/2 and 802.11 Standards

- **In HIPERLAN/2, medium access is based on a TDMA/TDD approach using a MAC frame with a period of 2ms**
- **This frame comprises of uplink (to the AP), downlink (from the AP), and direct link (DiL, directly between two stations) phases**
- **These phases are scheduled centrally by the AP, which informs stations at which point in time in the MAC frame they are allowed to transmit their data**
- **Time slots are allocated dynamically depending on the need for transmission resources**
- **The HIPERLAN/2 MAC is designed to provide QoS support, essential to many multimedia and real-time applications**
- **Another significant difference between the two standards is the length of the packets employed as HIPERLAN/2 employs fixed length packets, while 802.11a supports variable length packets**

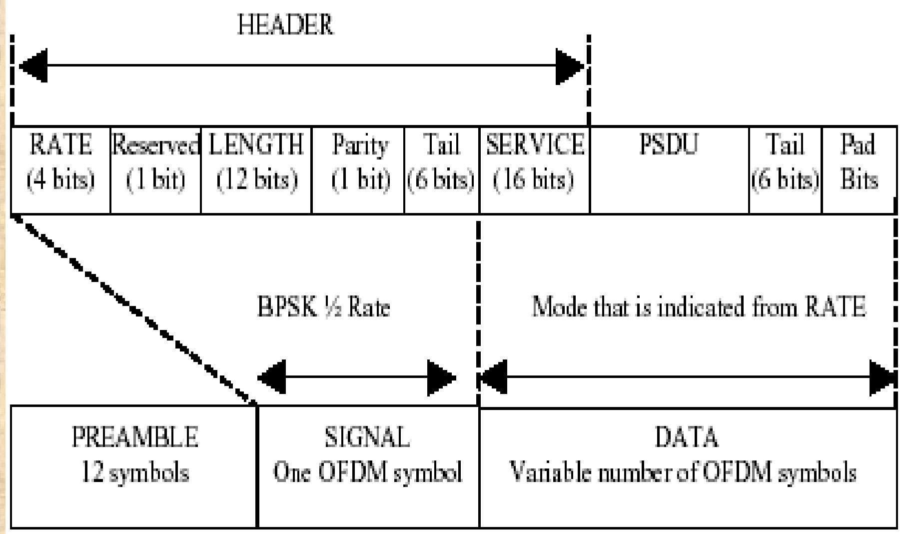
MAC Layer for HIPERLAN/2 and 802.11 Standard s



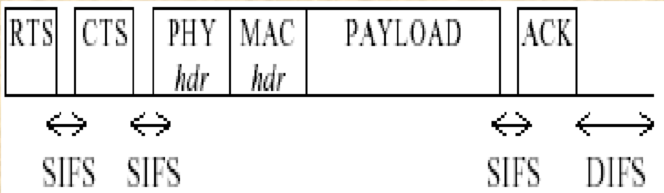
(a) – HIPERLAN/2 MAC frame



(b) – HIPERLAN/2 PDU format



(c) – 802.11a PDU format



(d) – DCF access mechanism

Conclusions and Future Directions

- The low cost of wireless LANs has led to a tremendous growth of its worldwide use
- Wireless LANs can be found in nearly all enterprise environments, in many homes, hotspots, airport lounges, among others
- Today, there is a high demand for the efficient support of multimedia applications over wireless LANs
- Needless to say that security is also a major concern
- IEEE is indeed addressing some of these aspects while the problem space is much larger
- The efficient utilization of the scarce radio resource is also an existing concern which needs more investigation, and cognitive and spectrum agile radios are attempts to address this issue
- Finally, integration of wireless LANs into the future integrated next generation heterogeneous networks beyond 3G is also a very hot topic
- Time to move to wireless PANs